jamk.fi

Tietoturvallisuuden kartoitus ja kehitys

Joonas Lipponen

Opinnäytetyö
Huhtikuu 2018
Tekniikan ja liikenteen ala
Insinööri (AMK), Tietotekniikan tutkinto-ohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Lipponen, Joonas	Opinnäytetyö, AMK	Huhtikuu 2018
	Sivumäärä 61	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Tietoturvallisuuden kartoitus ja kehitys

Tutkinto-ohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Sampo Kotikoski, Antti Häkkinen

Toimeksiantaja(t)
Pk-yritys

Tiivistelmä

Organisaatioiden tietoturvallisuuden tason kehittäminen on lähtökohtaisesti hankalaa ja toiminnan kehitykseen on hyvä ottaa yleisesti tiedossa olevia ja käytettyjä toimintaa tukevia viitekehyksiä. Taustana toimi kohdeorganisaatiossa harjoittelujakson aikana suoritettu tutkimus, josta syntyi idea kartoittaa organisaation tietoturvallista toimintaa tuotekehitysosastolla.

Tehtävänä oli tutkia kohdeorganisaation tietoturvallisuuden tasoa tuotekehityksessä ISO 27001-viitekehyksen mukaan. Tavoitteellisesti luotiin nykytilan analyysi tietoturvallisuuden hallintajärjestelmän vaatimuksista eli ISO 27001 standardista. Nykytilan analyysin perusteella valittiin yksi epäkohta, johon luotiin kehitysehdotus, joka tässä tapauksessa käsitti tietoturvakoulutuksen kehityksen.

Työ toteutettiin laadullisena tutkimuksena, jossa tietoa organisaation toiminnasta hankittiin avoimien haastatteluiden kautta sekä aikaisemman tutkimuksen perusteella. Tuloksena luotiin yleistason nykytilan arviointi, jossa käytettiin moniportaista arviointimenetelmää vaatimuksen täyttymisestä tuotekehityksen toiminnassa.

Kehitettiin tietoturvakoulutukseen perustasoehdotus sekä ehdotettiin koulutuskehyksen muodostamiseen mallia ja tapoja, joilla seurata koulutuksen suorituskykyä. Johtopäätöksenä voitiin todeta, että kyseisen viitekehyksen noudattaminen sinällään on raskas metodi pk-yritykselle sekä varsinkin näin varhaisessa vaiheessa toimivalle organisaatiolle.

Avainsanat (asiasanat)

Tietoturvallisuuden hallintajärjestelmä, ISO 2700x, riskinhallinta, hallintakeino

Muut tiedot (salassa pidettävät liitteet)
Liite 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 & 12,

jamk.fi

Description

Author(s)	Type of publication	Date
Lipponen, Joonas	Bachelor's thesis	April 2018
		Language of publication: Finnish
	Number of pages: 61	Permission for web publication: x

Title of publication

Gap analysis and development of information security

Degree programme

Information Technology

Supervisor(s)

Kotikoski Sampo, Häkkinen Antti

Assigned by

Small and medium-sized enterprise

Abstract

Developing the level of information security in organizations is principally difficult, and it is good practice to use commonly known and used frameworks for the development of information security. The background for this research was settled during an internship period, where the idea emerged to map out the organization's information security in the R&D department in more detail.

The task was to research the level of information security of the target organization in their R&D department according to the ISO 27001 framework. The aim was to create a current state analysis of the requirements regarding the information security management system, i.e. the ISO 27001 standard. Based on the current state analysis, one nonconformity was chosen for creation of a development proposal, which in this case included the development of information security training in the organization.

The study was carried out as a qualitative research where information of organizational activities based on a previous research was gathered through open interviews. As a result, an overall level of assessment was created using a multi-level evaluation method to analyze whether the R&D department meets the ISO 27001 requirement.

A proposal for a baseline regarding to information security training was developed, and for creating a training framework, a model and ways to monitor the performance of training were proposed. As a conclusion, the compliance with this kind of framework is a harsh method for a small and medium sized enterprise, and particularly for one operating in such an early-stage of its lifecycle

Keywords/tags (subjects)

ISMS, ISO 2700x, Information security, risk management, security control

Miscellaneous (Confidential information)

Appendix 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 & 12

Sisältö

Kuviot

Taulukot

Lyhenteet

CMM	Capability Maturity Model
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IJACSA	International Journal of Advanced Computer Science and Applications
ISO	International Organization for Standardization
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan, Do, Chech, Act
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

1 Lähtökohdat

1.1 Toimeksianto

Toimeksiantajana Jyväskylässä toimiva pk-yritys. Toimeksiannon ideana oli kartoittaa toimeksiantajan tietoturvallisuuden tasoa tietoturvallisuuden hallintajärjestelmän asettamien vaatimusten mukaan. Idea toimeksiantoon syntyi harjoitteluaikana luodusta nykytilan selvityksestä yrityksen verkkoinfralle, johon viitataan työssä. Yrityksessä tehdyn aikaisemman tutkimuksen puolesta heräsi idea tarpeeseen suorittaa kartoitus yrityksen riskienhallinnalliseen sekä toiminnalliseen tilaan laajemmin standardin mukaisen kehyksen pohjalta. Tavoitteena oli luoda analyysi yrityksen tilasta kohti yhteensopivuutta tietoturvallisuuden hallintajärjestelmän kanssa.

1.2 Tutkimusasetelma

Opinnäytetyön tutkimusongelma oli tutkia, millaiset valmiudet kohdeorganisaatiossa on tarkasteltavan standardin osalta omassa toiminnassaan noudattaa kyseistä viitekehystä. Tavoitteena oli myös löytää tietty epäkohta, johon pyrittiin löytämään standardin viitekehyksen mukainen kehitysehdotus. Tässä opinnäytetyössä käsiteltävä tutkimusongelma voidaan muotoilla muutamaan kysymykseen, johon työssä on pyritty löytämään vastaukset:

- Mitkä resurssit työntekijät käsittävät yritykselle tärkeiksi?
- Miltä osin yrityksen toiminta tuotekehitysympäristössä ei vastaa ISO 27001:n asettamia vaatimuksia?
- Miten kehittää tuotekehitysympäristön toimintaa ISO 27001:n vaatimusten suuntaisiksi?

Opinnäytetyö toteutettiin laadullisena eli kvalitatiivisena tutkimuksena, jossa aineiston kerätään toimintaympäristöstä haastatteluina. Haastattelut olivat avoimia ja teemoitettuja, jolloin riippuen haastateltavan asemasta yrityksessä, hankittavan tiedon teema vaihtuu. Tutkimusta varten haastateltiin sekä työntekijöitä, kuin myös organisaation asiantuntijoita ja johtoa.

Tuotekehitysosastolle tuotettava kysely kattaa hallintajärjestelmän hallintakeinojen mukaisien kehitys- ja ylläpitokeinojen noudattamista. Asiantuntijoille ja johdolle esitettävät kysymykset käsittelevät organisaation tietoturvallisuuden johtamista ja toimintaa.

Samaan teemaan kuuluvilta haastateltavilta kysyttiin likimain samat kysymykset. Ennen haastattelua haastateltaville toimitettiin alustavasti suunniteltu pohja, jonka mukaan haastateltava ymmärtää haastattelun tarkoituksen. Tulosten perusteella analysoitiin nykyinen valmiuden taso verrattuna ISO 27001-hallintakeinoihin ja vaatimuksiin. Rajaus suoritettiin nykytilanarvioinnin pohjalta, josta lähdettiin hakemaan tarkempaa näkökulmaa, mihin tietoturvan osaa-alueeseen kehitetään kehitysehdotus.

2 Tietoturvallisuus

2.1 Määritys

Tietoa voidaan luokitella erilaisiin kategorioihin riippuen siitä, kuinka tietoa säilytetään. Tietoa voi olla fyysisessä muodossa, kuten asiakirjat ja dokumentaatiot, sekä digitaalisessa muodossa kovalevyllä tai pilvessä tallennetuissa tiedostoissa. Tieto voi myös esiintyä aineettomana, kuten työntekijän tietotaidot. Tietoturvallisuudessa tieto voidaan ymmärtää etuna, jonka katsotaan olevan arvokasta, joka edellyttää asianmukaista suojaamista ja jonka asiattomasta suojaamisesta aiheutuu riskejä. Esimerkkejä yritykselle arvokkaista tiedoista voivat olla asiakas-, liiketoiminta-, yhteistyökumppani- tai henkilöstötiedot. (SFS-EN ISO/IEC 27000:2017,19.)

Tietoa välitetään muodosta riippumatta kohteelta toiselle kirjallisesti tai digitaalisesti, jolloin välityskeinosta riippumatta tulee tieto suojata. Tietoturvallisuuden voidaan sanoa varmistavan tiedon luottamuksellisuuden, käytettävyyden ja eheyden. Luottamuksellisuuden varmistaminen turvaa salassa pidettävän tiedon pysymisen salaisena, jolloin tietoon pääsee käsiksi vain siihen oikeutetut ihmiset. (Haruki, E 2017.)

Käytettävyyden varmistaminen mahdollistaa tiedon saatavuuden siihen oikeutetuille tahoille, halutulla ajalla ja tavalla. Eheyden varmistaminen kattaa tiedon aitouden, käyttökelpoisuuden, kattavuuden ja ajantasaisuuden. Lisäksi eheyden suojaaminen

varmistaa sen, että tietoa ei ole muutettu sen elinkaaren aikana ja että tietoa pystyvät muuttamaan vain ne tahot, joilla on siihen oikeus. (Haruki, E 2017.)

Tietoturvallisuuden tavoite on minimoida tietoturvahäiriöiden seuraukset mahdollisimman pieniksi ja näin ollen varmistaa organisaation liiketoiminnan menestyksekkään jatkuvuuden. Tätä varten tulee organisaatiossa ottaa käyttöön liiketoimintaan soveltuvia hallintakeinoja, jotka on valittu riskien hallintaprosessin avulla ja joita hallitaan myöhemmin selitetyllä tietoturvallisuuden hallintajärjestelmällä. (SFS-EN ISO/IEC 27000:2017, 20.)

2.2 Näkökulmat

Informaation suojaamiseen kuuluu sen laaja-alaisuudenkin takia monta eri näkökulmaa, jotka nivotaan tietoturvallisuudeksi. Tällaisia ovat mm. fyysinen-, laitteisto-, ohjelmisto- ja tietoliikenne turvallisuus, jotka käsittelevät teknistä ja fyysistä turvallisuutta toimintaympäristöissä. (VAHTI 3/2007, 59-69.)

Tietoaineistoturvallisuus käsittää erilaisten asiakirjojen, tiedostojen, tietoaineistojen sekä materiaalin käytettävyyteen, eheyteen sekä saatavuuteen vaikuttavia turvallisuusmekanismeja. Tärkeintä on suojata tietoaineistoa koko sen elinkaaren ajan. Tietoaineistojen turvaaminen lähtee luokittelumenetelmistä, joilla luokitellaan tiedon jakelu- ja suojausmenetelmät, kuten turvallisuusluokitus. Riippumatta siitä onko tietoaineisto fyysisessä tai sähköisessä muodossa tulee sille laatia turvalliset menettelyt tiedon säilytykseen, tiedonsiirtoon, käyttöön sekä hävittämiseen. (VAHTI 5/2004, 79-81.)

Henkilöturvallisuus käsittää käytännössä organisaation palveluksessa olevan henkilöstöön kohdistuvat turvallisuusmekanismit ennen, aikana sekä jälkeen työsuhteen. Ennen työsuhdetta turvallisuusnäkökulmana saattaa olla taustantarkastus sekä pätevyyden varmistaminen sekä myös henkilöstölle osoitettavia vastuita tietoturvallisuudessa esimerkiksi salassapitosopimuksen kautta. Työsuhteen aikana henkilöstöturvallisuus käsittää käytännössä työnkuvaan riittävät käyttö- ja pääsyoikeudet, perehdytyksen ja opastuksen henkilöstölle organisaation käytänteistä sekä kurinpidollisista asioista. Työsuhteen päättyessä henkilöstöturvallisuuteen kuuluvat työsopimuksissa sekä salassapitosopimuksissa määritetyt vastuut, jotka jäävät voimaan työsuhteen

päättyessä, sekä muut organisaation sisäisissä järjestelmissä olevien käyttöoikeuksien sekä kulkuoikeuksien hallinnointi. (SFS-EN ISO/IEC 27002:2017, 16-20.)

Käytännössä tietoturvallisuuden tukipilari on ylimmän johdon sitoutumisessa onnistuneeseen tietoturvan kehittämiseen ja organisointiin. Ylimmän johdon roolia ei voida liikaa korostaa tietoturvallisuuden tukipilarina organisaatioissa, koska vahvan sitoutumisen sekä johdon käytännön esimerkin kautta pystytään luomaan motivoitunut ilmapiiri yrityksen turvalliseen toimintaan ja näin ollen jalkauttamaan tietoturvallisen käyttäytymisen sitoutumista henkilöstöön. (VAHTI 5/2004, 27-32.)

Hallinnollinen tietoturva tähtää keinoihin, joilla luodaan tukipilarit organisaation tietoturvan onnistuneeseen johtamiseen, kehittämiseen sekä resurssointiin. Tällaisia keinoja ovat mm. tietoturvastrategia, politiikka, roolitus sekä koulutus. Strategian ja politiikan avulla ylin johto osoittaa organisaatiossa, sekä sidosryhmille tahdon ja sitoutuneisuutensa tietoturvallisen toiminnan jatkuvuuteen ja kehitykseen. Selkeän ja koko organisaation tasolla viestityn vastuunjaon kautta luodaan sujuva rakenne kyvykkääseen toimintaan. (VAHTI 5/2004, 27-32.)

Tärkeänä kohteena hallinnassa on osaamisen kehittäminen ja viestintä organisaation sisäisesti kuin ulkoisiin toimijoihin, koska nykypäivänä osaamista ja tietoisuutta tulee kehittää jatkuvasti, ja näin ollen johdon tehtävä on huolehtia henkilökunnan tietoturvallisuuteen liittyvän ajattelun ja osaamisen kehittämisestä. (SFS-EN ISO/IEC 27002:2017, 18-19.)

2.3 Arviointityökaluja ja nykyhetki

Business Continuity Instituutin teettämässä tutkimuksessa, jossa kartoitettiin yli 700 eri organisaation yli 70:stä eri maasta suurimpia uhkia ja häiriötekijöitä liiketoiminnalle vuonna 2017, juuri kyberuhka on suurin huolen aihe organisaatioissa (Horizon scan report, 2017). Tällöin organisaatioiden tulisi jatkuvasti arvioida liiketoiminnalle arvioitujen kyberuhkien vaikuttavuutta sekä implementoida sopivia menetelmiä tullakseen vastustuskykyisemmäksi mahdollisia kyberuhkia vastaan. Käyttämällä erilaisia arviointityökaluja pystytään analysoimaan organisaation kypsyyden tasoa turvallisuuden eri osa-alueilla. (Vogel, D 2017.)

Pinnalla olevia työhaluja viranomaisille ja organisaatioille tietoturvallisuuden auditointiin ja kehittämiseen ovat mm. KATAKRI ja VAHTI-ohjeistus. KATAKRI on kansallinen turvallisuudenauditointikriteeristö. Se perustuu voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvavelvoitteisiin (Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille).

VAHTI on valtiovarainministeriön asettaman julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, jonka luoma ohjeistus liittyy digitaalisen tietoturvallisuuden kehittämiseen ja ohjaamiseen (VAHTI-toiminnan organisointi n.d.). KATAKRI sekä VAHTI-ohjeistuksen määrittämät vaatimukset nähtiin tähän opinnäytetyöhön liittyvään kohdeorganisaation liian raskaiksi toteutettavaksi, jolloin kyseiset työkalut jätettiin käsittelemättä.

Euroopan Unionin laajuinen tietosuoja-asetus eli General Data Protection Regulation (GDPR) tulee voimaan keväällä 2018 se käsittää kaikki EU:n alueella toimivat yritykset, jotka prosessoivat ja käsittelevät henkilötietoja toiminnassaan riippumatta yrityksen sijainnista Euroopan Unionissa. Asetuksen myötä organisaatioissa tulee olla tietoisia kaikista sen keräämistä henkilötiedoista ja sen käsittelystä. Käytännössä asetus määrittää, mitä on henkilötieto, mitä velvollisuuksia henkilörekisterinpitäjällä sekä käsittelijällä on sekä minkälaisia sanktiota yritykselle on luvassa vaatimusten noudattamatta jättämisestä. (GDPR Key Changes n.d.)

Asetus yhdenmukaistaa tietosuojalainsäädäntöä EU:n alueella, mikä pienentää kitkaa eri jäsenmaiden välillä tapahtuvien palveluiden tarjoamisessa. Toisaalta asetus luo varmuutta palveluiden käyttäjälle siitä, että henkilötietoja käsitellään asianmukaisesti ja luottamuksellisesti riippumatta palveluntarjoajan lähtömaasta. Tietosuoja-asetusta ei tarkemmin käsitellä tässä kohdeorganisaatioon tehdyssä opinnäytetyössä.

3 Riskit tietoturvallisuudessa

3.1 Riskienhallinta

Riskillä tarkoitetaan jonkin odotetun tapahtuman poikkeamaa ja epävarmuuden vaikutusta haluttuihin päämääriin (VAHTI 22/2017, 11). Jokaiseen organisaation tekemään päätökseen ja toimintaan liittyy luonnollisesti riskejä. Riskejä ei luonnollisestikaan pysty täysin poistamaan, mutta niiden todennäköisyyttä voidaan pienentää ja vaikutusta pystytään supistamaan (Hakala, Vainio, & Vuorinen 2006, 90). Riskienhallinta voidaan ajatella prosessina, jossa organisaation johdon hyväksymää ja vastuulla olevaa riskien tunnistusta ja hallintaa toteuttaa koko organisaatio ja muu henkilökunta kaikessa toiminnassaan aina yrityksen strategian valinnasta asiakassuhteisiin. (Riskienhallinta Mistä riskienhallinnassa on kysymys n.d.)

Riskien luokittelutapoja on useita ja riippuen organisaation fokuksesta miten laajalla otannalla organisaatiossa lähdetään hallitsemaan riskejä, on myös riskit luokiteltava esimerkiksi liiketoiminnan kannalta vaikuttaviin strategisiin, operatiivisiin tai vahinkoriskeihin. Usein oikeassa elämässä riskien luokitteluun liittyy päällekkäisyyksiä. (Riskien luokittelu ja riskiesimerkkejä n.d.)

Pääasiassa 27001-standardin ydintavoite on organisaation riskienhallinta lähtien oman toimintaympäristön riskien tunnistamisella ja valitsemalla sopivimmat keinot, joilla hallita löydettyjä riskejä. Riskienhallinnalla pyritään löytämään potentiaalisia asioita, jotka saattavat vaikuttaa organisaation toiminnan jatkuvuuteen sekä tavoitteiden saavuttamiseen sekä negatiivisesti, että positiivisesti sekä löytämään sopivimmat keinot löydettyjen riskien neutraloimiseksi. Hallinta perustuu riskianalyysiin, johon kuuluvat riskin kartoitus ja arviointi organisaatiossa sekä vielä riskien käsittely. (Kosutic n.d.a.)

Riskien kartoitus sekä luokittelu perustuvat vahvalti ihmisten omiin kokemuksiin asioista, jolloin pitäydytään kartoittajan omaan tottumukseen eli päättelemisen mahdollisuuteen, mistä mahdolliset vaikutukset tai erot toimintaan juontuvat. Tällöin huomion keskipisteenä toimii totutun ympäristön havainnointi, jolloin epätodennäköisimmät ja odottamattomimman tapahtumat jäävät ns. sokeaan pisteeseen.

Taleb (2007) selittää kirjassaan *Musta Joutsen Erittäin epätodennäköisen vaikutus*, että se on vieras havainto, jota ei olla odotettu sekä sillä on äärimmäinen vaikutus. Alhaisen ennustettavuuden sekä suuren vaikutuksen ansiosta mustat joutsenet asettavat sen, mitä et tiedä suurempaan rooliin kuin sen, mitä tiedät. Mustien joutsenien tapahtuessa on siis keskitytty totutun ympäristön havainnointiin ja jätetty Nassim Talebin esittelemän Extremistanin vaikutukset huomiotta. (Taleb 2007, 15-17.)

3.2 Riskianalyysi

Riskianalyysi koostuu kahdesta vaiheesta: riskien kartoitus ja riskien arviointi. Kartoituksessa juonena on potentiaalisten riskien ja uhkakuvien löytäminen. Tämä voi tapahtua pohtimalla aikaisempien kokemusten kautta sattuneita ongelmia nykyhetkeen sekä miettiä, mitä haasteita tulevaisuus tuo tullessaan. Kattavan tuloksen saamiseksi on järkevää ottaa kartoitukseen mukaan mahdollisimman kattava osa organisaation henkilöstöä, joka toimii kartoitettavien järjestelmien ja toiminnallisuuksien parissa, kuin myös organisaation johtoa. (Hakala, Vainio, & Vuorinen 2006, 80-81.)

Kartoituksen jälkeen on vuorossa arviointi, jossa keskiössä on löydettyjen uhkakuvien ja riskien vaikutus organisaation toimintaan sekä realisoitumistodennäköisyyden arviointi. Arvioinnista lopputuloksena on yleensä dokumentaatio, johon todennäköisyys ja vaikutus sijoitetaan. Näin saadaan visuaalinen kuva, kuinka riskit jakautuvat, ja pystytään tekemään priorisointia helpommin, mitkä riskit ovat oleellisimpia organisaation päämäärien ja tavoitteiden kannalta. Luonnollisesti organisaation tulisi suhteuttaa arviointinsa toimialan, tavoitteiden sekä toimintakulttuurin mukaiseksi. (Curtis, & Carey 2012, 3-9.)

3.3 Riskien käsittely

Luonnollisestikaan kaikkia riskejä ei voida poistaa, mutta voidaan tehdä suunnitelma suurimpien uhkakuvien realisoitumisen välttämiseksi. Riskien käsittelyyn on olemassa erilaisia vaihtoehtoja riskin ottamisesta riskin siirtämiseen.

Varautumatta riskiin millään tavoin perustuu päätökseen hyväksyttävien riskien arviointikriteeristöön sekä johdon hyväksymien periaatteiden pohjalta. Tällöin tehdään

päätös implementoimatta hallintakeinoja ja ottamalla riski huolellisen harkinnan jälkeen. Riskin pienentäminen tapahtuu vaikuttamalla sen tapahtumatodennäköisyyteen tai vaikutukseen organisaation toimintaan implementoimalla hallintakeinoja. Organisaatiolla on myös mahdollisuus riskin ulkoistamisesta eli riskin siirtämisestä toiselle toimijalle. (Riskien hallinta: kehittämistoimenpiteet n.d.)

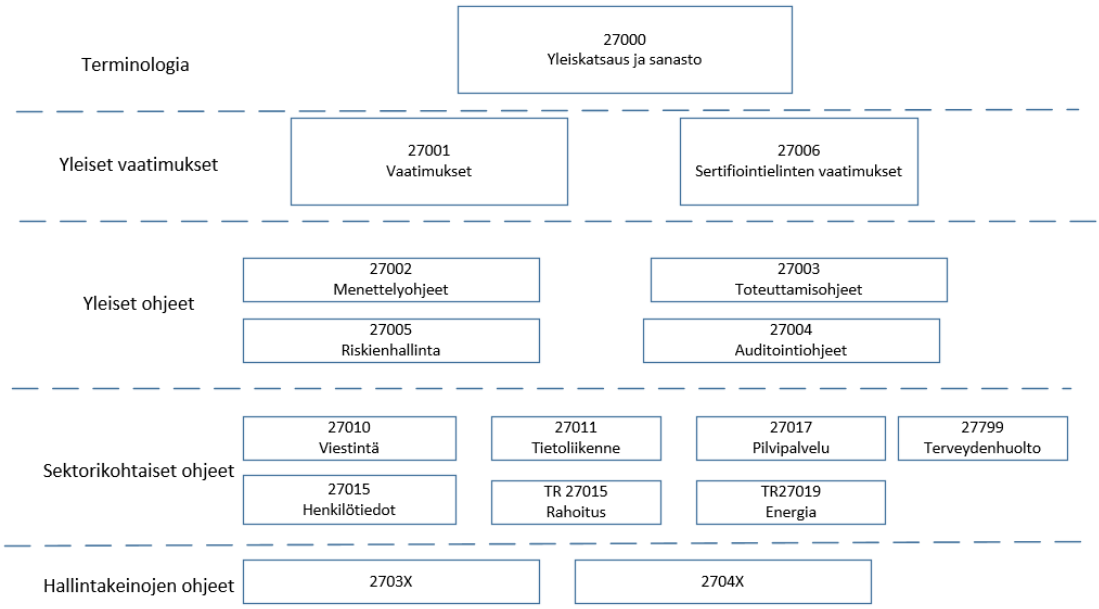
Tällöin tulee ottaa huomioon toimijan riskienhallintamenetelmät ja muistaa, että ulkoinen riski, jota ei hoideta ja hallita halutulla tasolla, on yhtä vakava kuin riski, joka olisi organisaation sisäisessä piirissä. Riskien siirrossa ulkopuolelle on myös huomioitava toimittajan turvallisuuden tason jatkuva seuraaminen. (Hakala, Vainio, & Vuorinen 2006, 90.)

4 ISO 27000 -standardiperhe

4.1 Yleistä

Kansainvälisen standardoitumiseen erikoistunut järjestelmän ISO (International Organization for Standardization) ja IEC (International Electrotechnical Commission) ylläpitämän 27000-standardiperheen tarkoitus on auttaa kaikentyyppisiä ja kokoisia organisaatioita toteuttamaan ja käyttämään tietoturvallisuuden hallintajärjestelmää. Standardiperhe koostuu terminologian määrityksestä, yleisistä vaatimuksista, yleisistä ohjeista, sektorikohtaisista ohjeista sekä hallintakeinojen ohjeista. (SFS-EN ISO/IEC 27000:2017, 5.)

Kuviossa 1 on kuvattu standardien välisiä suhteita ja osastointia.



Kuvio 1. ISO27000-standardiperhe (SFS-EN ISO/IEC 27000:2017, 26)

Mielenkiintoisimmat standardit työn tutkimusosan kannalta ovat ISO/IEC 27001 ja 27002, joista 27001 määrittelee tietoturvallisuuden hallintajärjestelmän luomiseen tarvittavat vaatimukset ja kontrollit sekä ylläpitoa ja jatkuvaa kehitystä koskevat vaatimukset. ISO27001-standardi antaa suuntamerkit organisaation tietoturvallisuuden hallintajärjestelmän luomiseen ja kertoo toteuttamiseen vaikuttavat organisaation tarpeet ja tavoitteet. (SFS-EN ISO/IEC 27001:2017, 5.)

4.2 ISO 27001

Käytännössä standardin avulla organisaatio pystyy luomaan tietoturvallisuuden hallintakehyksen, jolla se pystyy systemaattisesti hallitsemaan ja suojelemaan organisaatiolle tärkeitä tieto-omaisuuksia. Standardin rakenne noudattaa hyvinkin paljon PDCA (Plan, Do, Chech, Act) -mallia, mitä tulee tietoturvallisuuden hallintajärjestelmän implementointiin.

Kappaleet 4-7 määrittävät suunnitteluosuuden, jossa organisaation tulee esimerkiksi määritellä hallintajärjestelmän kattavuus sekä suunnitella tietoturvan tavoitteet ja tukitoiminnot. Kappale 8 kohdistuu implementaatio-osuuteen, jossa toteutetaan prosessit, joilla täytetään tietoturvavaatimukset.

Kappale 9 käsittelee tarkastusosiota, jossa keskitytään hallintajärjestelmän suorituskyvyn monitoroimiseen. Kappale 10 keskittyy jatkuvaan kehitykseen hallintajärjestelmän ympäristössä. Asiakirjan lopussa on myös Liite A, jossa on esitetty lukijalle hallintakeinoja, joista organisaatio voi valita hallintakeinoja järjestelmäänsä.

4.3 Tietoturvallisuuden hallintajärjestelmä

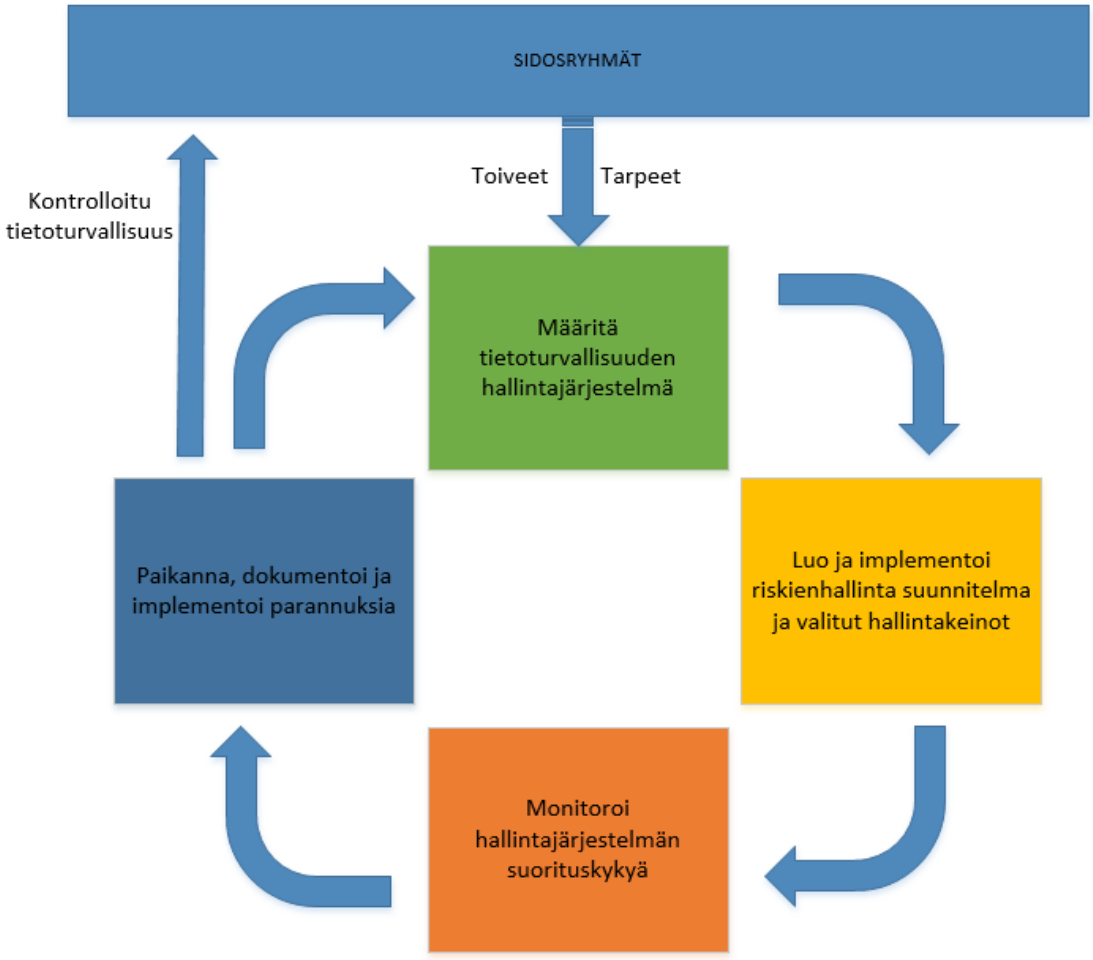
4.3.1 Yleistä

Tietoturvallisuuden hallintajärjestelmä voidaan kuvitella systemaattiseksi lähestymistavaksi hallita ja suojata yrityksen resursseja (Kosutic 2016). Tietoturvallisuus ei ole vain informaatioteknologian suojaamista, vaan se käsittää laaja-alaisesti organisaation eri toiminnan osa-alueita, kuten fyysinen turvallisuus, henkilöstöresurssien hallinta, oikeudelliset suojat, organisaation johtamisen ja politiikat.

Hallintajärjestelmän avulla pyritään hallitsemaan laaja-alaisesti organisaation tietoturvallisuutta havaitsemalla toimintaan liittyviä riskejä ja ottamalla käyttöön riskin käsittelyyn tarvittavia politiikkoja, prosesseja sekä määrittämällä tavoitteet niiden saavuttamiseksi.

Organisaation ylimmällä johdolla on omat vastuunsa tietotuvallisuuden hallintajärjestelmässä mm. määritellä liiketoiminnan odotukset tietoturvallisuudelle, esimerkiksi asettaa päämääriä liiketoiminnallisesti tärkeiden resurssien turvaamiselle. Johdon tulee laatia ja julkaista politiikat, kuinka hallita sitä, että asetetut tietoturvallisuuden päämäärät saavutetaan. (SFS-EN ISO/IEC 27001:2017, 7.)

Johdon tehtäviin kuuluu myös organisaatiossa vastuunjako, kuka on vastuussa ja mistä osa-alueesta kuin myös mahdollistaa tarpeeksi resursseja sekä rahallisesti, että henkilöstöresursseja, jotta hallintajärjestelmä saadaan toteutettua. Jatkuvan kehityksen takaamiseksi ovat katselmoinnit välttämättömiä, jotta pystytään arviomaan ja mittaamaan onko asetetut odotukset täytetty. Kuviossa 2 havainnollistetaan hallintajärjestelmän PDCA-mallisen jatkuvan kehityksen toiminnan vaiheet. (SFS-EN ISO/IEC 27001:2017, 7.)



Kuvio 2. PDCA-malli tietoturvallisuuden hallintajärjestelmästä (Hakala, Vainio, & Vuorinen 2006, 49)

4.3.2 Hallintajärjestelmän implementoinnin vaiheet

Määritys ja suunnitteluvaiheessa organisaation tulee määritellä hallintajärjestelmän kattavuus, eli mitä tietoa organisaation tulisi suojella. Oman toimintaympäristönsä ymmärtäminen sekä niiden ulkoisten ja sisäisten asioiden määrittäminen, jotka vaikuttavat organisaation kykenevyyteen saada haluttuja tuloksia hallintajärjestelmältä ovat keskeisessä osassa. (SFS-EN ISO/IEC 27001:2017, 6.)

Sisäisiä asioita voivat olla esimerkiksi liiketoimintastrategia, resurssit, tietojärjestelmät ja prosessit. Ulkoisia asioita voivat esimerkiksi olla sidosryhmien tarpeet ja vaatimukset, kuten oikeudelliset ja sääntelylliset vaatimukset, kilpailuympäristö ja mahdolliset poliittiset ja kulttuuriset vaikutteet. (Kosutic n.d.b.)

Standardin määritysten mukaan tässä vaiheessa organisaation tulisi määritellä ja dokumentoida tietoturvapolitiikka, jossa ylin johto määrittää toimintaperiaatteet sekä tarkoituksen, mitä tietoturvalla halutaan saavuttaa.

Riskien arvioinnin kautta organisaatio tunnistaa olemassa olevat riskit ja suorittaa riskien käsittelyprosessi, jossa valitaan riskien arvioinnissa esille tulleisiin riskeihin hallintamenetelmät ja keinot. Organisaation tulee dokumentoida soveltuvuuslausunto, joka ilmaisee, mitä hallintakeinoja organisaatio on valinnut riskienhallinta keinoiksi kuin myös perustelut mitkä hallintamenettelyt on jätetty pois. Organisaation tulisi määritellä tietoturvatavoitteet ja sekä säilytettävä dokumenttia tavoitteesta.

Suunnitteluvaiheeseen kuuluu myös täsmentää tukitoimintoja, kuten minkälaisia resursseja tavoitteet vaativat, millä tavoin viestitään sidosryhmien kanssa, minkä tasoinen pätevyys tietoturvallisuuden tasoon vaikuttavilla työntekijöillä kuuluu olla. Lisäksi kuuluisi määritellä periaatteet ja toimintatavat dokumentoidun tiedon hallintaan.

Implementointi vaiheessa organisaatio pistää käytäntöön suunnitellut hallintakontrollit ja riskienhallinta suunnitelman. Hallintakontrollien vaatimat järjestelmät, koulutukset, prosessit tulee laittaa käytäntöön tässä vaiheessa. (Calder & Watkins 2006, 36-37.)

Implementoinnissa tulee ottaa huomioon muutostenhallinta, koska tehtäessä suunniteltuja tai suunnitelmattomia muutoksia organisaatioon olisi pystyttävä ottamaan huomioon mahdolliset haittavaikutukset ja seuraukset muutoksille. Standardi ei määritä, että muutoksia tulisi dokumentoida, mutta parhaan lopputuloksen saamiseksi olisi hyvä ottaa käyttöön muutostenhallintamalli.

Onnistuneen implementointivaiheen jälkeen päästään suorituskyvyn monitorointiin, jossa tulisi tehdä dokumentaatiota, ovatko määritetyt hallintakeinot saaneet aikaan haluttuja tuloksia. Hallintajärjestelmän seuranta on toki jatkuva prosessi, johon tulisi

panostaa jo suunnittelu vaiheessa määrittelemällä mitä seurataan eli määritetyt organisaation toiminnot ja prosessit, kuin myös tietoturvallisuuden kannalta yritykselle kriittiset informaatiot. (SFS-EN ISO/IEC 27003, 116.)

Suorituskyvyn seurantaan liittyy myös seurantatavan määrittäminen, esimerkiksi viikoittaiset häiriöraportit. Organisaation tulee määritellä, kenen vastuulla seurannan toteutus on ja kuka analysoi saadut tulokset. Organisaatiossa tulisi myös ottaa käyttöön jaksottainen sisäinen auditointi tietoturvallisuuden hallintajärjestelmälle. Auditoinnissa tulee määrittä mitä osaa organisaatiosta lähdetään auditoimaan riippuen toki organisaation koosta, auditoidaanko koko yritys kerralla.

Tavoitteena auditoinnissa on saada selville hallintajärjestelmä vaatimusten mukainen ja ylläpidetty. Jos ei ole niin sisäisen auditoinnin raporttiin tulee raportoida löydetyt poikkeamat. Auditoinnissa tulisi varmistaa auditoijan puolueettomuus koskien mitä prosessia tai soveltamisalaa auditoijaan. (SFS-EN ISO/IEC 27001:2017, 13.)

Seurannasta saadut tulokset ovat tärkeitä hallintajärjestelmän kehittämisen kannalta. Tulokset seurannasta ja auditoinnista tulee dokumentoida sellaisella tarkkuudella, että ylin johto pystyy toimimaan tehtäviensä mukaisesti hallintajärjestelmän kehittämiseksi. (Kosutic n.d.c.)

Organisaation johdon tulee siis tehdä säännöllistä katselmointia saamistaan auditointien ja seurannan tuloksista kuin myös sidosryhmiltä saatuun palautteeseen liittyen tietoturvallisuuden tasoon. Johdon tulee käsitellä myös riskienhallinnan kautta implementoitujen hallintakeinojen soveltuvuus ja tavoitteiden täyttö.

Tietoturvallisuuden hallintajärjestelmän kehitysvaiheessa monitoroinnin tulokset analysoidaan ja dokumentoidaan löydetyt poikkeamat. Poikkeama tarkoittaa yleisesti tiedossa olevan tarpeen eli vaatimuksen täyttymättä jättämistä (SFS-EN ISO/IEC 27000:2017, 13). Esimerkiksi sidosryhmän tarpeiden ja odotusten täyttämättä jättäminen. Näihin poikkeamiin tulee organisaation reagoida korjaavilla toimenpiteillä. Poikkeamat sekä tehdyt korjaavat toimenpiteet ja niiden tulokset tulisi dokumentoida. Tulosten vaikuttavuuden dokumentointi on tärkeää, jotta organisaatio tietää, että onko juurisyy poikkeamaan löydetty ja onko sen uusiutuminen estetty. (SFS-EN ISO/IEC 27003:2017, 116-118.)

Organisaation tulee myös kehittää jatkuvasti hallintajärjestelmäänsä, jotta se on riittävä ja soveltuva toimintaympäristössä. Parantuvuuden taustalla on ajatus siitä, että toimintaympäristö, jossa organisaatio toimii, muuttuu jatkuvasti ja muutokset vaikuttavat myös tietoturvallisuuteen. Muutosten tapahtuessa myös riskit muuttuvat ja näin ollen hallintakeinojen vaikuttavuus muuttuu. (SFS-EN ISO/IEC 27001:2017, 13-14.)

Jatkuvan parantamisen kautta hallintajärjestelmällä tavoiteltua tietoturvallisuuden tasoa ja sidosryhmien tarpeita ja vaatimuksia täyttävää tietoturvaa ylläpidetään ajantasaisena.

4.3.3 Liitteen A hallintakeinot

Standardin liitteessä A on annettu 114 hallintakeinoa, joilla organisaatio pystyy hallitsemaan riskien arvioinnin perusteella löydettyjä riskejä. Kuten kappaleessa 3.4 mainittiin, soveltuvuuslausunto toimii dokumenttina, mitkä hallintakeinot otetaan käyttöön ja mitkä jätetään pois implementaatiosta. Hallintakeinot on jaoteltu 14 osioon A.5 – A.18, joissa on selitetty lyhyesti hallintakeinon sektori, mihin tietoturvallisuuteen liittyvään osa-alueeseen se liittyy sekä tavoitteet, mitä tällä kontrollilla tavoitellaan.

A.5 Tietoturvapolitiikat

Tämä osio käsittelee organisaation tietoturvapolitiikan luomista sekä jatkuvaa katselmointia. Tavoitteena on luoda organisaation tarpeen mukaan joukko johdon hyväksymiä tietoturvapolitiikkoja, kuten pääsynhallintaan, varmuuskopiointiin ja salaukseen. Myös tietoturvapolitiikkojen katselmointia tulisi aika-ajoin toteuttaa. (SFS-EN ISO/IEC 27001:2017, 15.)

A.6 Tietoturvallisuuden organisointi

Osiossa kontrollit tarjoavat keinoja organisaation sisäiseen tietoturvaroolitukseen ja vastuunjakoon, joilla luodaan hallintarakenne. Lisäksi hallintakeinoja organisaation etätyöskentelyyn ja mobiililaitteiden käytöstä syntyviin riskeihin. (SFS-EN ISO/IEC 27001:2017, 15.)

A.7 Henkilöstöturvallisuus

Tässä osiossa esitetään kontrolleja organisaation henkilöstön tietoturvallisuuteen-työsuhteen elinkaaren aikana, jossa käsitellään työntekijän velvollisuuksia ja vastuita ennen, aikana tai jälkeen työsuhteen sekä työsuhteen muuttuessa. Tavoitteena on siis varmistaa, että organisaatiossa työskentelevät ymmärtävät ja täyttävät vaatimukset, joita heille annetaan tietoturvan osalta. (SFS-EN ISO/IEC 27001:2017, 16.)

A.8 Suojattavan omaisuuden hallinta

Omaisuuksien hallinnan kontrollit käsittävät vastuunjaon sekä tietojen luokitteluun- ja käsittelyyn liittyviä hallintakeinoja. Kontrollien tavoitteena on luoda organisaatiolle käytännöt, miten arvokkaita tietoja käsitellään niille annettujen luokittelujen mukaan sekä dokumentaatio mitä ovat organisaation suojattavat omaisuudet. (SFS-EN ISO/IEC 27001:2017, 17.)

A.9 Pääsynhallinta

Osiossa ehdotettujen kontrollien tavoitteena on, että organisaatiossa luodaan ja toteutetaan pääsynhallinta politiikkaa, jolla estetään järjestelmien ja sovellusten luvaton käyttö sekä varmistaa vain valtuutettujen käyttäjien pääsy organisaation palveluihin ja järjestelmiin. (SFS-EN ISO/IEC 27001:2017, 18.)

A.10 Salaus

Salausosiossa pyritään luomaan organisaation periaatteita, joilla varmistetaan salattavan tiedon asianmukainen ja vaikuttava käyttö. Organisaation tulee päättää mitä tietoa tulee salata sekä luoda menettelyt salausavainten hallitsemiseen niiden elinikänä. (SFS-EN ISO/IEC 27001:2017, 19.)

A.11 Fyysinen turvallisuus ja ympäristön turvallisuus

Fyysisen turvallisuuden hallinnassa määritellään turva-alueilla työskentelyyn kuuluvia asianmukaisia kontrolleja, joilla estetään luvaton tunkeutuminen tietoaineistoihin ja käsittelypalveluihin. Osiossa annetaan lisäksi keinoja laitteistoturvallisuuteen, jotta organisaation omaisuus ei vaarantuisi. (SFS-EN ISO/IEC 27001:2017, 20.)

A.12 Käyttöturvallisuus

Käyttöturvallisuus osiossa annetaan kontrolleja IT-infrastruktuurin hallinnan osalta mm. muutosten- ja organisaation kapasiteetin hallintaan. Määritellään kontrolleja

haittaohjelmilta suojautumiseen, varmuuskopiointiin, kuten mitä varmuuskopioidaan ja kuinka usein, tapahtumien hallintaa kuten käyttäjien ja ylläpidon suorittamien toimintojen lokitukseen, tietojärjestelmien auditointiin sekä haavoittuvuuksien hallintaan. (SFS-EN ISO/IEC 27001:2017, 21.)

A.13 Viestintäturvallisuus

Viestintäturvallisuuden kontrolleilla pyritään hallitsemaan organisaation kaikentyyppisillä viestintäpalveluilla tapahtuvaa tiedonsiirtoa ja suojaamaan organisaation sisäistä tai ulkopuolisen osapuolen kanssa käytyä tiedonsiirtoa (SFS-EN ISO/IEC 27002:2017, 59). Hallintakeinoina esitetään mm. tiedonsiirtopolitiikan määrittely sekä salassapito- ja vaitiolositoumukset. Lisäksi organisaation tulisi pystyä valvomaan sekä luomaan turvamekanismeja verkkopalvelujen turvaamiseksi. (SFS-EN ISO/IEC 27001:2017, 22.)

A.14 Järjestelmien hankkiminen, kehittäminen ja ylläpito

Tässä osiossa määritellyillä hallintakeinoilla pyritään varmistamaan tietojärjestelmien turvallisuus niiden koko elinkaaren aikana hankkimisessa huomioitavista hyväksymiskriteereistä, kehittämistä koskevien sääntöjen, muutostenhallintamenetelmien sekä järjestelmä suunnittelun periaatteiden luomisella. (SFS-EN ISO/IEC 27001:2017, 24.)

A.15 Suhteet toimittajiin

Hallintakeinojen avulla ylläpidetään toimittajien kanssa tehtyjen sopimusten tietoturvallisuutta vaatimalla, miten toimittajien hallussa oleva suojattava omaisuus tulee suojata. Määritellään myös, että toimitettujen palveluiden tarjoamia muutoksia tulee hallita ja katselmoida. (SFS-EN ISO/IEC 27001:2017, 24.)

A.16 Tietoturvahäiriöiden hallinta

Standardin 27000-määritelyt mukaan tietoturvahäiriö on

> ”*Yksi tai useampi epätoivottu tai odottamaton tietoturvatapahtuma, joka suurella todennäköisyydellä vaarantaa liiketoiminnot ja uhkaa tietoturvallisuutta*.” (SFS-EN ISO/IEC 27000:2017, 11)

Tietoturva häiriöiden hallinnan kontrolleilla pyritään määrittämään hallintavastuut sekä kuinka häiriöistä ja heikkouksista tulisi raportoida organisaatiossa. Kontrolleilla

käsitetään myös häiriöiden ratkaisuun ja reagointiin liittyviä toimia kuten dokumentaatio. (SFS-EN ISO/IEC 27001:2017, 25.)

A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Organisaation tulisi määritellä tietoturvallisuuden jatkuvuuden suunnittelu, toteutus ja jatkuva kehitys määrittelemällä vaatimukset, miten dokumentoidaan ja ylläpidetään tietoturvallisuuden prosesseja ja hallintamekanismeja sekä todentaa mekanismien vaikutus. Lisäksi kontrolli tietojenkäsittelypalveluiden vikasietoisuuden varmistaminen.

A.18 Vaatimustenmukaisuus

Osiossa määritellään organisaation vastuulle noudattaa kaikkia tietoturvallisuuteen liittyvä lakeja ja säädöksiä toiminnassaan sekä dokumentoitava toimintamalli niiden vaatimusten täyttämiseksi. Immateriaalioikeuksien piiriin kuuluvien ohjelmistojen vaatimuksien noudatus sekä kuinka tallenteiden suojaaminen tulisi toteuttaa. Lisäksi henkilötietojen käsittelyä suojaaminen ja tietoturvapolitiikan katselmointiin liittyviä hallintakeinoja.

Kuten liitteen rakenteesta huomataan, tietoturvallisuudesta vain osa on IT-teknologian turvaamista ja käsittää laajemmin tietoturvallisuuden mm. johdon sitoutumisen tietoturvallisuuteen ja menettelyjen ja politiikkojen määrittämisen organisaatioon. Lisäksi on paljon dokumentoinnissa ja organisaation toimintatavoissa huomioitavia asioita. Kokonaisedellytykset tietoturvallisuudelle luodaan yrityksen toimintatavoilla ja hyvin määritellyllä ylläpidolla ja kehittämisellä, johon ylin johto antaa edellytykset ja tuen.

4.4 ISO 27002

ISO 27002-standardi, tietoturvallisuuden hallintakeinojen menettelyohjeet, jolla organisaatio voi valita hallintakeinoja ISO27001-standardin toteuttamisprosessiin tai organisoida käyttöönsä yleisesti tunnustettuja tietoturvallisuuden hallintakeinoja sekä mahdollisesti kehittää omaa hallintaohjettaan. (SFS-EN ISO/IEC 27002:2017, 8.)

Käytännössä standardi on tarkoitettu tarkempaa tarkastelua varten tietoturvallisuuden hallintajärjestelmän implementointiin. Näin ollen standardi kertoo yksityiskohtaisemmin ISO27001-standardissa liitteessä A määritettyjen hallintatavoitteiden- ja keinojen toteuttamisohjeet. (Kosutic n.d.d.)

Mainitut toteutusohjeet ovat vain lähinnä suuntaa antavia eivätkä välttämättä sovi täysin organisaation tavoitteisiin hallintajärjestelmälle, jolloin organisaation tulee itse soveltaa riittävä toteutusmenetelmä omaan ympäristöönsä. Lisäksi kansainvälinen standardi tarjoaa lisätietoja mahdollisiin muihin standardeihin viittauksissa tai lakiteknisiin asioihin hallintakeinon toteutuksessa. Standardi tarjoaa tutkimustyön kannalta hyviä menettelyohjeita, joilla täytetään kehitysehdotus osiota

5 Tutkimushaastattelut

5.1 Haastattelujen tarkoitus

Haastattelut suoritettiin erikseen tuotekehitysryhmälle ja yrityksen johtohenkilöille. Tuotekehitysryhmälle suoritetuilla haastatteluilla pyrittiin luomaan käsitystä millaisia resursseja työntekijät käsittävät yritykselle tärkeiksi ja näin ollen luomaan pohjaa millaisten resurssien tietoturvallisuuteen tulisi panostaa. Lisäksi haastattelussa pyrittiin hakemaan työntekijöiden omia havaintoja tietoturvaan liittyen omassa toimintaympäristössään. Tuotekehitysryhmän haastattelussa pyrittiin keskittymään järjestelmien ja laitteiston turvallisuuteen sekä tietoturvahäiriöiden hallintaan, kuin myös työskentelytapoihin.

Yrityksen johdolle luomissa haastattelukysymyksissä käsitellään tietoturvallisuuden johtamista ja hallintaa, esimerkiksi miten organisaatiossa on otettua huomioon ympärillä oleva toimintaympäristö, kuinka organisaatiossa on tällä hetkellä ylläpidetty riskienhallintaa ja kuinka tietoturvallisuutta kehitetään.

Yrityksen tuotekehitysyksiköstä haastateltiin noin tusinan verran henkilöstöä. Haastateltaville toimitettiin kysymykset etukäteen, jotta haastateltava osaisi valmistautua

tilanteeseen. Haastattelut suoritettiin yksilöhaastatteluina, jotka tallennettiin ja litteroitiin. Päätettiin haastatella koko tuotekehityksen parissa työskentelevät henkilöt kokonaiskuvan saamiseksi. Tekstimuotoisista haastatteluista muodostetiin tiivistelmät, jonka pohjalta lähdettiin tekemään yhteenvetoa haastatteluista saatuja tuloksia. Haastattelussa esitetyt kysymykset ovat liitteestä 1.

5.2 Tuotekehityksen haastattelujen yhteenveto

Eräs tutkimuskysymys oli mitä resursseja työntekijät käsittävät yritykselle tärkeiksi. Haastattelujen pohjalta tuli esille salattavaksi ja tärkeiksi tiedoiksi koettiin tuotekehityksessä kehitettävän ohjelmiston lähdekoodi sekä asiakasmateriaali, joka voi olla dataa, henkilötietoja tai dokumentteja ja lisäksi yrityksen sisäinen kommunikaatio käsittäen yrityksen viestintäkanavat (Liite 2, 3, 4, 5, 6 ,7 & 8.).

Toimintaympäristössä olevia tietoturvariskejä on havainnoitu mm. fyysisten laitteistojen sekä dokumenttien suojaamisen osalta. Esille tulleita asioita olivat toimipisteellä säilytettävien tärkeiden dokumenttien säilytys lukitsemattomassa tilassa sekä sen, että sisäänkäynnin ovi ei aina mene kiinni vaan lukko jumiutuu. (Liite 5, 8, & 11.) On havaittu myös muiden työntekijöiden välinpitämättömyyttä määritettyjen selainlisäosien käyttöä sekä työaseman lukitsemista kohtaan, kun et ole fyysisesti läsnä. Esille tuli myös muistivälineillä olevien salassa pidettävien tiedostojen hallinnan puutteita. (Liite 6.)

Toimintaympäristössä sijaitsevaan palvelimeen pääsee käsiksi kolme henkilöä, joista yhdellä on palvelimen varmuuskopioinnin vastuu. Lisäksi palvelimen käyttöoikeuksien jakoon ei ole erityisiä järjestelyjä. Kysyttäessä palvelimen varmuuskopioinnista ja sen vastuutuksesta tuli ilmi epäselvyyksiä, kuten kenen vastuulla se on ja tapahtuuko sitä edes. Todellisuudessa varmuuskopiointia tapahtuu manuaalisesti, mutta ei hallitusti ja kopioiden koestaminen puuttuu. Palvelinta, jossa tärkeitä resursseja sijaitsee ei varmuuskopioida järjestelmällisesti sekä palvelimen fyysinen lukitus, sekä keskitetty sijainti nähtiin ei niin tietoturvallisena vaihtoehtona. (Liite 4, 5, 6, 8 & 11.)

Toimintaympäristössä suurin osa käyttää salasanatietojen hallintaan salasananhallinta ohjelmistoa. Haastattelujen perusteella omaa muistikapasiteettia käytetään myös tunnistetietojen hallintaan (Liite 7).

Asiakkaalta saatujen laitteistojen tietoturvallisuudesta ei tullut ilmi selkeätä ohjeistusta tai toimintatapaa, kerrottiin kuitenkin hyviä käytänteitä mm. tunnistautumistietojen hallintaan sekä fyysiseen laitteiston hallintaan.

Tietoturvatapahtumista viestitään toimintaympäristössä Microsoft Teams:n ryhmäviestintä ohjelmiston kautta tai sähköpostin avulla. Toimintaympäristössä ei ole käytössä tietoturvahäiriöiden ilmetessä käytettävää toimintasuunnitelmaa, vaan tapahtumista viestitään vapaasti käyttäen edellä mainittuja kanavia ja vastuuhenkilö vastaa ratkaisusta. (Liite 4, 5, 6 & 7.)

5.3 Johdon haastattelujen yhteenveto

5.3.1 Sitoutuminen ja viestintä

Haastattelujen perusteella ylimmän johdon sitoutumista tietoturvallisuuteen on tapahtunut mm. nimittämällä vastuuhenkilö, joka on edesauttanut tietoturvan kehittämistä projektiluontoisesti. Yritykseen on myös luotu palveluryhmä, jonka tehtävänä on viestittää tietoturvallisuuteen liittyvistä asioita sekä kehittää yrityksen tietoturvallisuutta. (Liite 3, 9 & 10.)

Haastattelujen perusteella tietoturvallisuuteen kuuluvista sidosryhmien tarpeiden huomioinnissa nousi esille asiakasyhteydet. Varsinaisia vaatimuksia ei asiakkaiden suunnalta tule vaan toimintaa ohjaa salassapitosopimuksen kautta asiakkaan omat tietoturvapolitiikat ja käytänteet, jotka jalkautetaan asiakasyhteyshenkilön avulla projektin toimintaan. (Liite 3, 9, 10 & 12.)

Organisaation ulkopuolelle käytävää yrityksen tietoturvallisuuteen liittyvää viestintää ei käydä toistaiseksi. Kävi ilmi, että toimintaan tulee muutoksia, näin ollen ulkoisen viestinnän organisointi sekä millaista viestintää tarvitaan, tulee kysymykseen tarkemmin. Yrityksen sisäisestä viestinnästä tietoturvallisuuden osalla vastaa nimetty vastuuhenkilö, joka käyttää yrityksen omia viestintäkanavia asioiden ilmi tuomiseen. Johdon näkemyksen mukaan organisaation viestintätapa tietoturvallisuuden tärkeydestä perustuu yrityksen tietoturvakoulutukseen, joka tapahtuu pikimmiten työsuhteen alkaessa sekä nimetyn tietoturvallisuuden vastuuhenkilön kautta. Keskitettyä

viestintää ei ole vaan yrityksen palveluryhmän henkilöt vievät asioita eteenpäin omiin osastoihinsa. (Liite 9 & 10.)

5.3.2 Riskienhallinta

Organisaatioon on tehty kertaluontoinen riskikartoitus, jonka pohjalta luotu äskettäin palveluryhmä. Organisaation johdon mukaan riskienhallinnallinen näkökulma tällä hetkellä on liiketoiminnallisissa riskeissä, jolloin keskiössä on yrityksen tavoitteisiin vaikuttavien riskien ratkominen. (Liite 3, 9 & 12.)

Tarkempaa juuri tietoturvallisuuteen liittyvää riskikartoitusta ei olla tehty organisaatiossa, mutta on tunnistettu riskialueita liittyen yrityksen sisäisiin- ja asiakkaiden tietoihin liittyen, joihin on toimenpiteitä suunnitteilla. Tietoturvariskien käsittely on tällä hetkellä ad hoc tyylistä eli erillistä käsittelysuunnitelmaa ei ole ja toimenpiteet tehdään suoraan riskin havaittaessa. Tietoturvariskien käsittelystä vastaa käytännössä yksi valtuutettu henkilö organisaatiossa. (Liite 3 & 9.)

Riskienhallinnasta vastaavan palveluryhmän toiminta on keskittynyt aikaisemman auditoinnin tuloksena syntyneisiin toimenpiteisiin, jonka myötä yritykseen on nimetty myös riskienhallintavastaava. Jo aiemmin mainitun riskikartoituksen tuloksena on syntynyt dokumentointi riskeistä, sekä nimetty riskin omistajat, arvioitu todennäköisuus, prioriteetti ja rahallinen kustannusarvio riskin vaikutuksista. (Liite 10, 11 & 12.)

5.3.3 Tukitoiminnot

Tarkempaa tietoturvallisuuteen vaadittavaa resurssointia ei olla tehty organisaatiossa, vaan lähestymistapana on se, että tarpeen vaatiessa lisätään resurssointia. Haastateltavien mukaan tietoturvallisuuden resurssointiin valtuutetulle henkilölle on annettu valtuudet hankkia näin katsoessaan tarvittavia työkaluja ja välineitä. (Liite 9 & 10.)

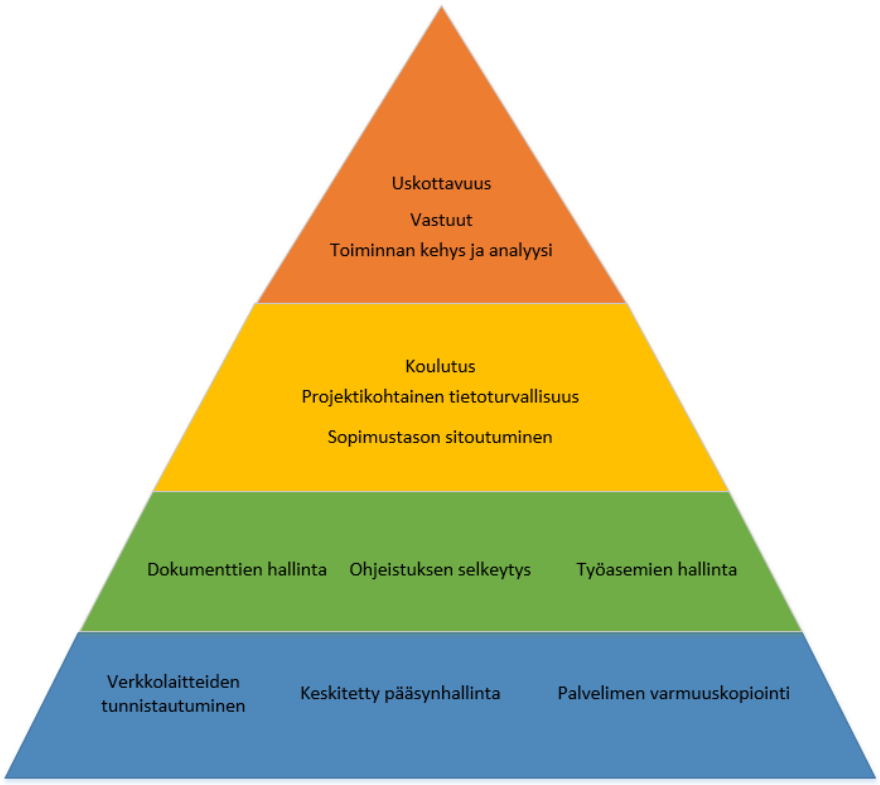
Yrityksen toiminta tietoturvallisuuteen vaikuttavien henkilöiden pätevyyden varmistamiseen käytetään tietoturvakoulutusta, josta jää merkintä koulutusrekisteriin. Pätevyyden määrittelyä tapahtuu rekrytoinnissa, jolloin luotetaan silloisen HR-

asiantuntijan näkemykseen sekä erikseen vielä tuotekehityksessä toimivan ryhmän arviointikykyyn

Organisaatiolla ei ole selkeää tavoitetilaa tietoturvan kehitykselle, vaan tietoturvaa kehitetään, projektinomaisesti tällä hetkellä. Sisäisiä auditointeja ei järjestetä tietoturvallisuuden kehittämiseksi vaan toiminta on myös projektinomaista. Ensimmäinen sisäinen auditointi, mitä yritykseen on järjestetty, tapahtui hiljattain, joka käsitteli yrityksen käytänteitä. Kehitysasiat ovat tosin käsiteltävissä kuukausittain palveluryhmän kokouksissa. Organisaatiossa ei ole haastateltujen mukaan käytössä sellaisia prosessimaisia menetelmiä, joiden arviointi tai analysointi mahdollistaisi erillistä seurantaa prosessien suorituskyvystä.

5.4 Kehityskohteet

Haastatteluissa pyydettiin haastateltavien näkemystä, mihin painopisteisiin henkilöstössä panostettaisiin enemmän tai mitä lähtisivät kehittämään oman toimintaympäristönsä tietoturvallisuuden osalta. Kuvioon 3 on muodostettu pääpiirteittäin esille tulleita aiheita kehitykseen, jotka on luokiteltu organisaation ylemmän tason toiminnallisuuksista alemman tason käytännön tekemiseen.



Kuvio 3. Kehitysehdotuksia toimintaan asteittain

Ylemmän tason kehityskohteena oli oman uskottavuuden kehittäminen kyberalalla toimijana, jonka näkemyksenä on se, että tietoturvallisuus toimii liiketoiminnan ajurina. Uskottavuuteen liittyen asennekasvatukselle nähtiin myös tarvetta, kun puhutaan asiakastiedon suojaamisesta, johon liittyy organisaation maineen ylläpito.

Haastateltavien näkemyksen mukaan tämän hetkiset järjestelyt tietoturvavastuiden osalta vaatii kehittämistä, nähtiin että liikaa vastuita on kasattu yhdelle vastuuhenkilölle niin tietoturvallisuuden määrittämisen kuin johtamisen kannaltakin. Roolitusta tulisi järkeistää kehitystyön osalta, koska tällä hetkellä asiakastyössä olevat eivät pääse antamaan täyttä panostaan. Yrityksen toimintaan vaadittaisiin sisäistä analyysiä, missä pisteessä mennään, jota verrataan, johonkin toimialan hyväksi katsomaan kehykseen, jonka kautta syntyisi kehitystoimenpiteitä.

Haastatteluissa nousi esille yrityksen sisäisen koulutukseen koko organisaation tasolla, kuten esimerkiksi seurantaosuus tämän hetkisen kertaluontoisen koulutuksen lisäksi kuin myös riskienhallinnallista koulutusta palveluryhmälle. Organisaatiossa on

käynyt ilmi aikaisemman tutkimuksen perusteella, että riittävää pätevyyttä ei kaikilla työntekijöillä ole, mitä tulee päivittäiseen tietoturvalliseen käyttäytymiseen. Näin ollen vaaditaan tukea riittävän pätevyyden takaamiseksi. (Tuotantoverkon tutkimus ja kehitys 2017.)

Esille nousi myös asiakkaiden kanssa tehtyjen palvelusopimusten vaatimusten täyttymisen epävarmuus nykyisessä dokumenttien hallinnan mallissa. Huolena oli, että toimituskohtaisien sopimusten vaatimaa luottamuksellisuuden tasoa ei pystytä varmistamaan, johon vaadittaisiin sitouduttujen toimitussopimusten läpikäynti organisaatiossa.

Projektityöskentelyssä nähtiin, että puuttuu kirjalliset ohjeet toimitusprojekteihin, sekä yksittäisen projektin käytänteisiin sekä turvallisuusvaatimuksiin keskittyvää perehdyttämistä ei suoriteta henkilöstölle suunnitellusti.

Tuotekehityksen toimintaympäristössä nousi esille luottamuksellisten dokumenttien hallintaan liittyviä kehityskohteita, kuten mahdollisten sähköisten tietovälineiden sisältämän asiakastiedon huolimaton hävitys turvallisella tavalla. Toimitiloissa sijaitsevien vapaasti saatavilla olevat mahdollisesti luottamuksellista tietoa sisältävien dokumenttien säilytys koettiin turvattomaksi ratkaisuksi, lisäksi henkilöstön työasemilla käsiteltäviin mahdollisesti luottamuksellisien dokumenttien käsittelyä tulisi parantaa.

Osallaan haastateltavien mielestä nykyiset käytänteet ovat joissain määrin työtä rajoittavia ja niitä tulisi selkeyttää esimerkiksi lisäosien kannalta on huomattu käyttöongelmia, jonka kautta suositeltuja lisäosia ei välttämättä käytetä. Myös määrittelytasoihin haluttaisiin selkeyttä, kuten mikä on riittävä salauksentaso tiedolle sekä selkeämpää ohjeistusta työssä käytettävän laitteiston käyttöön ja säilytykseen. Turvallisiksi määritettyjen menetelmien käytöstä tulisi jatkuva aikaisesti muistuttaa henkilöstöä, vaikka jatkokoulutuksen muodossa.

Haastateltavien mukaan kehityskohteita ovat työasemien hallinnan lisääminen nimenomaan päivitysten osalta, joka tällä hetkellä on käyttäjän vastuulla. Haastattelujen myötä tuli ilmi, että toimintaympäristössä olevan palvelimen tietoturvallisuuden ylläpitoon halutaan lisää pätevyyttä.

Pääsynhallinnallisesti yrityksessä ei ole keskitettyjä menetelmiä, jolloin on henkilöstöä käyttää monia käyttäjätunnus salasana -pareja, joten tämä saattaa aiheuttaa jatkossa ongelmia työsuhteiden tai tehtävien muuttuessa. Tuotekehitysympäristössä nähtiin myös kehityksen kohteena verkon aktiivilaitteiden tunnistautumismenetelmien käyttö, jota tällä hetkellä ei harjoiteta. Käyttöturvallisuuden kannalta kehitettävää on toimintaympäristössä sijaitsevan palvelimen suojattavien resurssien varmuuskopiointi, joka tulisi saattaa kuntoon automaattiseksi sekä luotettuun tilaan, joka nykyisillään tapahtuu manuaalisesti ja suunnittelemattomasti.

5.5 Päätelmiä

Yhteenvetona voisi vetää toiminnan olevan joissain määrin epäjärjestelmällistä eli suunniteltavuus on vähäistä toistaiseksi. Asiakkaiden tarpeet nähdään, mutta osataanko suhteuttaa työntekijöiden pätevyys vaadittuun tietoturvallisuuden tasoon. Aikaisemmin tuotetussa kyselyssä kävi ilmi, että määritettyjen käytänteiden noudattaminen ei ole itsestäänselvyys työntekijöiden keskuudessa, lisäksi tämä tutkimus tukee ajatusta käytänteiden ja ohjeistuksen selkeyttämiselle. (Tuotantoverkon tutkimus ja kehitys 2017). Riittävää pätevyyttä ei kaikilla yrityksen työntekijöillä ole toisaalta määritettyä henkilöstön pätevyyden perustasoa ei ole selkeästi rajattu.

Tämän hetkinen organisaatio ei kokonsa puolesta välttämättä vaadi niin suurta määrää dokumentoituja politiikkoja ja menettelyohjeita, jolloin esimerkiksi pääsynhallinta ja tietoturvahäiriöistä tiedotus suoritetaan organisaation omia ei niin strukturoituja käytänteitä.

Työntekijöiden keskuudessa nähdään, että ohjeistus on joissain määrin työtä rajoittava, mikä altistaa niiden noudattamatta jättämiselle. Organisaation tietoturvallisuuden organisoinnissa on jätetty paljon yhden työntekijälle vastuulle, kuten tietoturvaan liittyvä resurssointi, ylläpito, operatiivinen viestintä, tietoturvariskien arviointi ja käsittely sekä mahdollisten sidosryhmien tarpeiden hoito. Näin ollen suunnitelmallinen ja strukturoitu ote puuttuu vaadittujen resurssien varmistamiseen.

Näin ollen roolituksen osalta syntyy pullonkaula, toki yrityksen henkilöresurssien määrä vaikuttaa asiaan. Haastattelujen pohjalta yrityksen kypsyys jatkuvalle tietoturvallisuuden mittaamiseen, seurantaan ja analysointiin ei ole toistaiseksi viitekehykseen nähden riittävä.

6 Nykytilan arviointi

6.1 Arviointimenetelmä

Organisaation toiminnan täyttyvyyttä standardin vaatimuksiin nähden tullaan arvioimaan taulukon 1 kuvaamien tasojen mukaan. Asteikkoon on otettu mallia prosessien kypsyysmallista eli Capability Maturity Model (CMM), jonka alkuperäisenä tarkoituksena on kuvata ohjelmistokehityksen prosessien kypsyystasoa. Käytetään moniasteista luokittelua, tarkemman kuvan saamiseksi vaatimuksen täyttymisestä. Taulukoissa käytetty otsikointi on ISO 27001:2013 standardin klausuulien mukainen.

Taulukko 1. Vaatimuksen valmiuteen käytettävä asteikko

Taso	**Selitys**
1. Puuttuva	Toiminta on suunnittelematonta tai luonteeltaan epäjohdonmukaista. Epäjärjestyneisyyttä vaatimuksen täyttämisessä.
2. Alustava	Vaatimus on alustavan suunnitelman tasolla. Toiminta on muodollista.
3. Määritetty	Toiminta on suunniteltua ja organisaatio suorittaa vaatimuksen täyttävää prosessia.
4. Hallinnoitu	Vaatimuksen päämäärän saavuttamista hallitaan ja katselmoidaan. Suorituskykyä arvioidaan.
5. Optimoitu	Vaatimuksen suorituskykyä optimoidaan vastamaan nykyistä ja tulevaisuuden tarpeita.

6.2 Tietoturvallisuuden suunnittelu

6.2.1 Organisaation toimintaympäristö

Lainsäädännöllisesti ainakin tietosuoja-asetuksen huomiointia on, yrityksen toimialankin puolesta. Haastattelujen perusteella kanta huomioinnin riittävyyteen on vaihteleva, joidenkin mielestä asetus ei kosketa toimintaa ja joidenkin mukaan on valmistauduttu huonosti asetukseen ja sen vaikutuksiin, määrittelyä on siis tehty haastattelujen perusteella, analyysin riittävyydestä on eriäviä mielipiteitä. Mitä tulee muihin lakisääteisiin säädöksiin, niin haastattelujen perusteella yrityksessä luotetaan siihen, että johto, lakiasiamies sekä muut esimiehet ovat asiantuntemuksellaan ottaneet huomioon niiden vaikutukset.

Organisaatiossa ei olla selkeästi formalisoitu spesifiä tavoitetilaa tietoturvallisuudelle, joten juuri tavoiteltuun tulokseen vaikuttavia asioita on hankala määritellä. Organisaation tarkoituksen kannalta on huomioitu liiketoiminnallisen turvallisuuden merkitys, jota tukee palveluryhmän perustaminen sekä riskikartoitusten teettäminen.

Yrityksen kasvaessa taloudellisia tekijöitä on otettu huomioon mm. kilpailuympäristö, jota ei haastateltavien perusteella ei vaikuttavasti ole sekä kasvavan laitekannan hallittavuus. Tietoturvallisuuden kannalta saatavilla olevaa resurssointia ei olla merkittävästi määritetty, vaan resurssointia tehdään tarpeen määrittämän mukaan.

Tarkempaa määrittelyä toimintaympäristön sidosryhmistä ei olla tehty, mutta tarpeiden huomiointi keskittyy asiakkaiden kanssa tehtyihin salassapitosopimuksiin, jolloin huomiointi tapahtuu projektitasolla asiakasyhteyshenkilön kautta. Haastatteluista käy ilmi, että tarpeiden ja odotusten jalkautusta tietoturvan osalta ei spesifisen projektien kohdalla tehdä henkilöstölle. Haastattelujen ja Tuotantoverkon tutkimus- ja kehitystutkimuksen perusteella henkilöstön tarpeiden huomiointi esimerkiksi käytänteiden kehityksen osalta on kehitysvaiheessa.

Yrityksessä ei olla määritelty soveltamisalaa hallintajärjestelmälle, vaan oletusarvoisesti tietoturvallisuus koskee kaikkia yrityksen osa-alueita. Näin ollen standardin määrittämää hallintajärjestelmän rajausta, luomista, ylläpitoa sekä parannusta ei ole tapahtunut, vaan toiminta perustuu yrityksen tietoturvallisuuden kehittämiseen, joka

tällä hetkellä on liiketoimintariskien hallintapohjaista. Taulukossa 2 on arvioitu yrityksen toimintaympäristöön liittyviä vaatimuksia pohjautuen yllä mainittuihin kertomuksiin.

Taulukko 2. Organisaation toimintaympäristö

Organisaation toimintaympäristö	
Organisaation ja sen toimintaympäristön ymmärtäminen	2
Sidosryhmien tarpeiden ja odotusten ymmärtäminen	2
Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen	1
Tietoturvallisuuden hallintajärjestelmä	1

Jotta organisaatio pystyttäisiin määritellä Organisaation toimintaympäristö-klausuulien vaatimusten mukaiseksi, tulisi määritellä, mitä tavoitteet yrityksen tietoturvallisuudelle, jotka ovat linjassa strategisiin liiketoimintatavoitteisiin. Tämän hetkisten mahdollisuuksien analysointi myös resurssoinnin sekä roolitusten ja vastuiden kautta avaisi näkemyksiä asioille, jotka vaikuttavat haluttujen tavoitteiden täyttymiseen.

Sidosryhmien vaatimusten ymmärtämiseksi tulisi selvittää tehtyjen palvelusopimusten vaatimukset ja suhteuttaa ne omiin tietoturvallisuuden määrityksiin. Erillistä dokumentaatiota ei vaadita määrittelyn lisäksi sisäisistä tai ulkoisista asioista, mutta vaihtoehtoinen menetelmä voi olla esimerkiksi PESTE-analyysi yrityksen poliittisesta, ekonomisesta, sosiaalisesta ja teknisestä tilasta.

Soveltamisalan määrittämiseen tulisi rajata, mitä osia organisaatiossa halutaan hallintajärjestelmän piiriin esimerkiksi prosesseissa, tieto- ja viestintätekniikassa sekä fyysisesti toimipaikoittain. Soveltamisalalla pyritään ottamaan huomioon aikaisem-

min määritettyjen vaatimukset sekä tarpeet suunniteltaessa rajapintoja ja riippuvuussuhteita ulkomaailmaan organisaatiosta. Tästä pitäisi luoda standardin mukaan dokumentaatio, josta käy ilmi selkeästi ja tarkasti dokumentoitu hallintajärjestelmän kattavuusalue.

Tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja ylläpitoon ja parantamiseen vaaditaan hallintajärjestelmän luomista, joka edellyttää johdon hyväksyntää hallintajärjestelmä projektille, josta luotujen toimintaperiaatteiden noudattamista ja kehittämistä vaalitaan ISO 27001-vaatimusten mukaisesti.

6.2.2 Johtajuus

Organisaatiossa toimivan ylimmän johdon varmistuksella on valtuutettu vastuuhenkilö tietoturvallisuuden operatiiviseen toimintaan, jonka johdolla yritykseen on luotu tietoturva käytänteitä. Tällä hetkellä organisaation käytössä olevat tietoturvakäytänteet ovat pitkälti käytännön tekemiseen laadittuja ohjeistuksia eivätkä näin ollen täytä tietoturvapolitiikan kriteeristöä, tosin se antaa perustan tietoturvatavoitteiden operatiiviseen näkökulmaan.

Lisäksi organisaatioon on muodostettu palveluryhmä, jonka tehtävänä on toiminnan kehittäminen sekä mm. riskienhallinnallisesti. Näin ollen ylimmän johdon sitoutuminen näyttäytyy myös valtuutettujen tekeminä toimina. Johdon varmistamaa yhtenäisen sekä selkeää tavoitetilan asetusta tietoturvallisuudelle ei ole säädetty. Organisaation tavoitetilaa on selkeyttänyt aikaisemmin teetetty tutkimus yrityksen käytänteistä sekä käynnissä olevan auditoinnin kautta.

Formaaleja prosesseja yrityksessä on verrattain vähän, ja joihin olisi tietoturvallisuuden vaatimuksia yhdistettävissä on lähinnä työkoneiden ylläpidolliset asiat, joidenka varmistaminen on olematonta toiminnan perustuessa luottamukseen, että yrityksen menetelmillä ja säännöillä toimitaan.

Yrityksen koon myötä henkilöresursseja tietoturvan kannalta keskeisiin rooleihin on vähän, tällöin käytännön operointi on yhden valtuutetun henkilön vastuulla ja johdon mukaan tälle toiminnalle ei ole nimellistä tarvekattoa budjetissa. Muita roolituksia organisaatiossa on tehty mm. nimittämällä riskienhallintavastaava.

Organisaatiossa toistaiseksi viestitään tietoturvallisuuden tärkeydestä työsuhteen alussa järjestettävässä koulutuksessa, jonka jälkeen laadittujen vaatimusten noudattamisen tärkeydestä viestitään sattumanvaraisesti yrityksen kommunikointiväyliä käyttäen vastuuhenkilön kautta. Koulutuksen kautta henkilöstön tulisi tietää mikä on heidän panoksensa suojellessaan informaatiota työskennellessään yrityksessä.

Johdon tukemaa jatkuvaa kehittämistä tapahtuu palveluryhmän toimien määrittelemissä rajoissa. Menetelmiä, joilla johto varmistaa henkilöstön ohjautuvan tietoturvallisuuden kehittämiseen ei ole määritelty. Taulukossa 3 on esitetty arviointi organisaation johtajuuden tasosta liittyen johtajuuden vaatimuksiin standardissa.

Taulukko 3. Organisaation johtajuus

Johtajuus	
Johtajuus ja sitoutuminen	2
Tietoturvapolitiikka	1
Organisaation roolit, vastuut ja valtuudet	2

Johtajuus-klausuulisen täyttämiseksi ylimmän johdon organisaatiossa tulisi osoittaa sitoutumista varmistamalla, että mm.

- Tietoturvapolitiikka, sekä tietoturvatavoitteet laaditaan
- Standardin vaatimusten integraatio organisaation prosesseihin
- Resurssien saatavuus
- Haluttujen tulosten saavuttaminen

Tulisi siis laatia dokumentoituna organisaation tarkoituksen, strategian, sekä toiminta-ajatuksen mukainen tietoturvapolitiikka, joka määrittelee myös yrityksen tietoturvatavoitteet. Ylimmän johdon tulisi luoda menetelmä, jolla se ohjaa henkilöstöä

hallintajärjestelmän kehittämiseen, näin ollen olisi johdon pystyttävä selvästi ilmaisemaan mitä maaleja tietoturvallisuudelle on asetettu ja millä strategialla sinne päästään.

Tietoturvallisuuden kehittämisen tukemiseksi tulisi esimerkiksi määritellä menetelmät, joilla seurataan haluttujen tulosten saavuttamista. Organisaatiossa tulisi määritellä mitä resursseja se vaatii tietoturvallisuuden ylläpitämiseksi ja varata budjettiin tarvittavat henkilö- aika- ja raharesurssit. Roolien ja vastuiden osalta tulisi järkevöittää nykyistä yhden miehen ratkaisua jakamalla nykyistä kuormaa resurssien puitteissa.

6.2.3 Suunnittelu

Organisaatiossa on muodostettu palveluryhmä, jossa riskienhallinta on yhtenä toiminnan osa-alueena. Yrityksessä on tunnistettu riskikartoituksen kautta kriittisiä riskialueita kuten asiakkaiden tietoturva sekä yrityksen sisäiset kohteet. Riskeihin liittyvien toimenpiteiden suunniteltavuus on vielä kehitysvaiheessa sekä mahdollisten toimien seuranta tapahtuu palveluryhmän kokouksissa. Tietoturvallisuutta suunniteltaessa tulisi organisaatiossa ottaa huomioon aikaisempien määriteltyjen sidosryhmien tarpeet, jota tällä hetkellä tapahtuu projektikohtaisten sopimusten näkökulmasta.

Nimenomaista tietoturvariskien arviointia suoritetaan palveluryhmän toiminnassa. Organisaatiossa riskienhallinta perustuu liiketoimintalähtöisten riskien tunnistamiseen, jossa tietoturvariskit ovat yksi osa-alue. Toistaiseksi tietoturvariskien osalta hallinta on tunnistamisen sekä toimenpiteiden suunnittelun tasolla, eli tarkempaa analysointia ja arviointia ei suoriteta.

Yrityksessä käyttöönotettu toimintatapa liittyen riskien arviointiin käsittää kuukausittaiset palveluryhmän kokoukset, jossa tunnistetaan uusia riskejä sekä hallitaan aikaisempia toimenpiteitä. Uusia riskien tunnistaessa riskille nimetään juurisyy, riskin omistaja, arvioitu todennäköisyys sekä vaikutus, toimenpiteet ja aikataulu. Toimenpiteiden kehitystä seuraa nimetty laatuvastaava. Toistaiseksi dokumentoitua tietoa arviointiprosessista on kokouspöytäkirja.

Tietoturvariskien käsittelyyn ei olla suunniteltu ja määritetty erillistä prosessia tai suunnitelmaa. Tutkimusta tehdessä tietoturvariskeihin liittyvät toimenpiteet olivat suunnitteilla, sekä operatiivisten tietoturvariskien ilmentyessä niiden hallinta tapahtuu ns. ”ad hoc” tyylisesti tarpeen vaatiessa ja riskiin räätälöidyllä ratkaisulla. Erillistä soveltuvuuslausuntoa, mitä hallintakeinoja on valittu ja miksi ei ole, vaan organisaatiossa on käytössä oma riskianalyysipohja, johon kirjataan valitut keinot riskin käsittelyyn.

Organisaation tietoturvatavoitteita on selkeyttänyt aikaisempi auditointi, josta noussut esille nykytilan arviointi sekä riskienhallinnan kehitys. Johdon mukaan yleisesti ottaen liiketoiminnallisten riskienhallinnan kautta on haluttu ylläpitää liiketoiminnan jatkuvuutta sekä kyberturvallisuus alalla toimivan yrityksen maineen säilymistä. Organisaatiossa on tunnistettu tärkeitä suojeltavia kohteita, jonka mukaan on laadittu käytänteitä kohteiden suojelemiseksi.

Kuten aikaisemmin mainittu selkeät tietoturvallisuuteen liittyvät tavoitteet ovat organisaatiossa määrittelemättä näin ollen niiden saavuttamiseksi tarvittavien toimien suunnittelua on hankala spesifioida. Taulukossa 4 on arvioitu tämän hetkistä tasoa tietoturvariskien hallinnan suunnittelusta.

Taulukko 4. Suunnittelun arviointi

Suunnittelu	
Riskien ja mahdollisuuksien käsittely	
Yleistä	3
Tietoturvariskien arviointi	2
Tietoturvariskien käsittely	1
Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	1

Suunnittelu-klausuulien vaatimusten täyttämiseksi tulisi luoda tietoturvariskien arviointiprosessi, jossa tunnistetaan, analysoidaan ja arvioidaan tietoturvariskit. Tämän hetkisestä arvioinnista tulisi jäädä dokumentaatio, josta käy ilmi arviointimetodien kuvaus sekä arvioinnin tulokset. Tulisi terävöittää riskienkäsittelyn suunniteltavuutta eli olisi luotava käsittelysuunnitelma sekä käsittelyyn laadittava prosessi, jonka tulisi ottaa huomioon arvioinnista saadut tulokset sekä sidosryhmien, että toimintaympäristön tarpeet sekä pohtia miten riskien käsittelyä koskevasta hallinnasta viestitään.

Lisäksi tulisi laatia soveltuvuuslausunto, mitä hallintakeinoja on standardin Liitteestä A jo implementoitu, valittu tai jätetty valitsematta sekä mitä ulkoisia hallintakeinoja on otettu mukaan. Soveltuvuuslausunnossa tulisi myös ilmetä miten hallintakeino on implementoitu ja missä vaiheessa implementointi on.

6.2.4 Tukitoiminnot

Tietoturvallisuuden toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen varattavia resursseja nykyisessä kokoluokassa olevan organisaation toimintaan on vähän, esimerkiksi organisaatiossa ei ole IT-osastoa, jolle resurssointia pystyttäisiin tekemään. Tietoturvallisuuden resursointiin yrityksessä on vastuuhenkilö, jolle on annettu oikeudet hankkia tarvittavia resursseja yrityksen sisäisen tietoturvallisuuden ylläpitoon ja kehitykseen. Tarkempaa määrittelyä ajan, rahan tai tarvittavien mekanismien osalta ei ole selkeästi määritelty ja varattu toimintaan.

Riittävän pätevyyden määritys perustuu jo työnhaku vaiheessa arvioitavaan ammatilliseen pätevyyteen sekä koulutuksen tuottamasta tiedosta yrityksen käytänteisiin. Pätevyyden varmistamiseksi yrityksessä järjestetään uusille työntekijöille tietoturvallisuuskoulutus yrityksen sisäisiin käytänteisiin, josta jää merkintä koulutusrekisteriin. Koulutus on luonteeltaan kertalaatuinen, eli jatkuvaa kouluttamista ei organisaatiossa pidetä. Aikaisemmin teetetty tutkimus osoitti, että kaikilla työntekijöillä ei ole tarvittavaa pätevyyttä, mitä tulee käytänteiden noudattamiseen, joten tämän hetkinen pätevyyden tason nostatusta tai käytetyn ohjeistuksen muuttamista työhön sopivaksi. (Tuotantoverkon tutkimus ja kehitys 2017.)

Koulutuksen ja perehdytyksen kautta työntekijöiden pitäisi olla tietoisia yrityksen käytänteistä ja käytössä olevasta kurinpitomenettelystä. Siitä miten työntekijät voivat osaltaan vaikuttaa tietoturvallisuuden parantamiseen kehotetaan keskustelemaan viestintäkanavia pitkin.

Yrityksen tietoturvallisuuteen olennaista viestintää käydään viestintäkanavia pitkin, keskitettyä kanavaa informoimiseen ei olla säädetty. Viestinnän hoitaa tietoturvallisuuden vastuuhenkilö, joka tekee päätöksen, miten viestitään tietoturvallisuuteen liittyvissä asioissa.

Dokumentoitua tietoa, jota standardi ISO 27001 vaatii ylläpidettäväksi ei nimellisesti ole. Organisaatiossa on määritetty sisäiset käytänteet, koulutusrekisteri sekä riskikartoituksen kautta tunnistettu liiketoiminnallisia riskejä, joita on listattu. Yrityksessä vielä käynnissä kehitys, jonka kautta se tulee vielä määrittämään tarkemmin, millaisia dokumentteja se katsoo tietoturvallisuuden kannalta tärkeää ja välttämättömäksi.

Yrityksessä on käytössä oma asiakirjapohja, sekä dokumentoidun tiedon salassapito luokitus, jonka mukaan dokumentteja jaetaan asianomaisille. Dokumentteja ylläpidetään myös pilvipalveluissa, jossa käytetään palvelun tarjoamia menetelmiä, tiedon jakeluun sekä pääsynhallintaa. Ei ole tiedossa onko varmistettu pilvipalvelussa säilytettävien eri asiakasdokumenttien salassapitosopimusten määrittämää luottamuksellisuuden tasoa.

On myös havaittu, että tuotekehityksen toimipisteellä luottamuksellisia dokumentteja säilytetään kaikille työtilassa asioivien ihmisten ulottuvilla. Dokumenttien hävitykseen ei olla säädetty tiettyjä mekanismia, jolloin asianomainen hävitys saattaa jäädä tapahtumatta. Taulukossa 5 on arvioitu yrityksen tukitoimintoja sekä dokumentoidun tiedon hallintaa.

Taulukko 5. Tukitoimintojen arviointi

Tukitoiminnot	
Resurssit	1
Pätevyys	2
Tietoisuus	2
Viestintä	2
Dokumentoitu tieto	
Yleistä	2
Dokumentoidun tiedon luominen ja päivittäminen	2
Dokumentoidun tiedon hallinta	2

Tukitoiminto-klausuulien vaatimusten täyttämiseksi resurssien osalta tulisi määritettävä ja varattava ylläpitoon ja kehitykseen tarvittavat resurssit eli toisin sanoen organisaation pitäisi pystyä määrittämään suunniteltujen haluttujen tulosten analyysin pohjalta, mitä sisäisiä resursseja sillä on jo käytettävissä sekä järkevöittää nykyistä roolitusta esimerkiksi lisäämällä henkilöresursseja tietoturvallisuuden johtamiseen ja operatiiviseen toimintaan.

Pätevyyden kehittämiseksi tulisi luoda ja määrittää mikä on organisaation henkilöstön riittävä ja ylläpidettävä pätevyyden perustaso. Menetelmiä, joilla riittävä perustaso saavutetaan esimerkiksi koulutussuunnitelmalla sisäisen jatkuvan koulutukseen sekä mahdollistaa motivoitu henkilöstön itse ylläpidettävä osaaminen tietoturvallisuuden osalta. Lisäksi tarvittavan tason seuraamisen täyttymistä olisi hyvä seurata.

Henkilöstön tietoisuutta tulisi kasvattaa organisaation toimintatavoista ja menetelmistä, jotta organisaatiossa vallitsisi ymmärrys, miksi halutun tietoturvallisuuden tason saavuttaminen on tärkeää. Tietoisuus siitä miten henkilöstö pystyy omalta osaltaan vaikuttamaan tietoturvantason kehittämiseen, voidaan kompensoida koulutussuunnitelmassa ottaen huomioon järjestettävillä keskustelutilaisuuksilla tai luomalla toimintaympäristö, jossa henkilöstöllä on matala kynnys keskustella kehitettävistä asioista.

Viestinnän osalta tulisi määritellä mahdollisesti viestintäprosessi sekä keskitetty menetelmä mitä viestitään kelle ja miksi sekä mikä on organisaation kannalta tärkeää viestintää niin ulkoisesti ja sisäisesti.

Dokumentoidun tiedon osalta tulisi pystyä tarkentamaan ja terävöittämään henkilöstölle riittävät menetelmät luottamuksellisten sähköisten ja fyysisten tietojen ja asiakirjojen säilytykseen sekä hävittämiseen. Lisäksi mahdollisten muiden sopimusperäisten tietojen hallintaan liittyvää kartoitusta.

6.3 Tietoturvallisuuden toteuttaminen

Organisaatiossa toimeenpantu riskienhallinta toiminta on ollut käynnissä suhteellisen lyhyen aikaa, joten dokumentoitua tietoa siitä onko saavutettu suunnitelmien mukaisia tuloksia, on vielä vähän. Yrityksen toimintamallissa osa työntekijöistä toimii asiakkaanympäristössä asiakkaan laitteilla, joten käytännön tietoturvallinen toiminta mukautuu asiakkaan vaatimuksiin. Tietoturvaan vaikuttavia prosessimaisia toimia ovat tietoturvakoulutus sekä työkoneiden ylläpidolliset menetelmät. Työkoneiden ylläpidolliset toimet ovat olleet työkoneen käyttäjän itsensä vastuulla ja se on todettu olevan kestämätön ratkaisu, joten toimeenpano on tältä osaa ei ole täydellistä.

Yrityksen toiminta-ajatus liittyen tietoturvalliseen toimintaa perustuu luottamukseen, sekä siihen että sovituista käytänteistä pidetään kiinni ja toimitaan niitten mukaisesti, näin ollen varmuutta asetettujen tapojen täyttymiseen ei ole nykyisessä ratkaisussa.

Tuotekehitykseen liittyvät tietoturvalliset menetelmät sekä käytänteet on ohjeistettu koulutuksen kautta, jolloin esimerkiksi työkoneiden salauksen toteutuminen on luottamuksen piirissä. Tuotekehityksessä käsitellään yrityksen liiketoiminnan kannalta kriittisiä tietoja, jolloin toiminnan salaus- ja pääsynhallinta menetelmiin on keskitytty enemmissä määrin. Haastattelujen perusteella kehitystoimenpiteitä nimenomaisesti pääsynhallinnan sekä sähköisen sekä fyysisen tiedonhallinnan kanssa on kehitettävää.

Tietoturvariskien arvioinnin osalta on tunnistettu riskejä sekä toimenpiteitä, jotka ovat suunnitteilla. Suurempia suunnitelmia tietoturvariskien käsittelyyn ei toistaiseksi

vielä ollut, niin suunnitelman mukaista käsittelyä ei olla toimeenpantu tai tällä hetkellä se on ad hoc-tyylistä. Taulukossa 6 on esitetty toiminnan arviointi.

Taulukko 6. Toiminnan arviointi

Toiminta	
Toiminnan suunnittelu ja ohjaus	2
Tietoturvariskien arviointi	1
Tietoturvariskien käsittely	1

Toiminnan suunnitteluun ja ohjakseen vaadittua organisaation tietoturvavaatimusten täyttämiseksi vaadittujen prosessien osalta esimerkiksi käytänteiden osalta tulisi tehdä evaluaatiota miltä osin asioita pitäisi kehittää, jotta haluttuja menetelmiä todella käytetään. Tietoturvariskien osalta arviointia tulisi pystyä tekemään suunniteltuin aikavälein. Tietoturvariskien käsittelyyn tulisi laatia suunnitelmallinen pohja ja pyrkiä toteuttamaan sen määrittämien hallintakeinojen mukaan. Arvioinnista ja käsittelystä tulisi jäädä dokumentaatio niiden tuloksista.

6.4 Tietoturvallisuuden seuranta

Organisaation kypsyyteen nähden toimintaan on nidottu erittäin vähän minkäänlaista mittarointia tai seurantaa liittyen tietoturvallisuuden suorituskyvyn arviointiin. Organisaatioon on tehty aikaisemmin yksi sisäinen auditointi ulkopuolisella työvoimalla liittyen tietoturvallisuuteen. Suunniteltua sisäistä auditointia ei siis suoriteta yrityksessä. Johdon katselmointia ei tapahdu niinkään suunnitelluin aikavälein, haastattelujen mukaan johdon tietämys heidän vastuistaan on kuitenkin kasvanut aikaisempien auditointien myötä. Taulukossa 7 on arvioitu organisaation oman tietoturvallisuuden suorituskyvyn arviointia.

Taulukko 7. Suorituskyvyn arviointi

Suorituskyvyn arviointi	
Seuranta, mittaus, analysointi ja arviointi	1
Sisäinen auditointi	1
Johdon katselmus	1

Suorituskyvyn arviointiin organisaatiossa tulisi pohtia ja määrittää, mitkä asiat ovat tarkoituksenmukaisesti seurattavissa. mm. hallintakeinoista ja prosesseista. Arvioinnin perusteella seurataan ovatko valitut menetelmät tuottaneet haluttuja tuloksia suhteessa siihen, mitä tavoitteita organisaatiossa on. Lisäksi tunnistettavien muutosten kautta voidaan luoda jatkuvaa kehitystä kokonaisuuden kannalta. Organisaation sisäinen auditointiohjelma on myös eräs keino seurata, miten vaikuttavasti hallintajärjestelmää on ylläpidetty toteutettu. Johdon katselmusten osalta olisi harkittava, mikä on riittävä katselmoinnin taso organisaatiossa, jotta mahdollinen palaute, muutokset sekä parantamisen mahdollisuudet saadaan käsitellyksi johtoportaassa.

6.5 Tietoturvallisuuden kehitys

Toiminnassa tietoturvallisuuteen liittyviin poikkeamiin reagoidaan heti vastuuhenkilön toimesta, joka luo tarvittavat toimenpiteet ja menetelmät poikkeaman neutralisoimiseksi. Toimenpiteiden arviointia sekä niiden vaikuttavuutta ei vastuuhenkilön oman harkintakyvyn lisäksi suoriteta. Dokumentoitua tietoa poikkeaman luonteesta tai siihen tehtyjen korjaavien toimenpiteiden tuloksista ei luoda tai säilytetä. Taulukossa 8 on esitetty arviointi organisaation tietoturvallisuuden parantamisen kykyyn.

Taulukko 8. Kehityksen arviointi

Parantaminen	
Poikkeamat ja korjaavat toimenpiteet	2
Jatkuva parantaminen	1

Klausuulien mukaiseksi toimintaan pitäisi pystyä strukturoimaan poikkeamista johtuvien tai muutosten aiheuttamia kehitystoimenpiteitä. Aikaisemmin valittuja korjaavia ja ehkäiseviä hallintakeinoja tulisi yhdistää suunniteltuun katselmointiin ja sisäiseen auditointiin niiden tehokkuuden tasosta.

Näin organisaatio pystyy demonstroimaan tietoturvallisuuden jatkuvaa parantamista. Vaihe vaatii selkeät ja määritellyt mittarit ja arvioinnin perusteet aikaisemmasta vaiheesta halutuista avainprosesseista sekä hallintakeinoista. Esimerkiksi kypsyysmallien käyttämisellä voidaan kartoittaa prosessien ja hallintakeinojen suorituskykyä kohti laadukasta ja kontrolloitua tietoturvan tasoa sidosryhmille.

7 Kehitysehdotus

Luodun tutkimuksen perusteella organisaation tietoturvallisuuden kehittämisen näkökulmia on vielä monia, johtuen juurikin yrityksen voimakkaasta kasvutilasta ja kypsyystasosta määritellä päämääriään sekä resurssivajeesta tietoturvallisuuden toiminnan ja tietoturvallisen toimintakulttuurin jalkauttamisessa ja kehityksessä.

Henkilöstön panostus on oleellisen vaikuttava osa koko yrityksen tietoturvallisuuden toteutumisen kannalta. Henkilöstön tietoisuus siitä, miksi on tärkeää päivittäisessä työskentelyssä ottaa huomioon yleinen ja ennen kaikkea organisaation oma turvallisuusnäkökulma on saavutettavissa koulutuksen, opastuksen ja keskusteluiden avulla.

Nykyisen toiminnan tason kehittämiseksi katsotaan parhaaksi tietoturvakoulutuksen kehitysehdotus, koska organisaatiossa ei ole määritelty pohjatasoa, jota ylläpidettäisiin sekä seurattaisiin. Tavoitteena on kehittää nykyistä koulutussuunnitelma, jossa pyritään luomaan perustaso henkilöstön päivittäiselle tietoturvalliselle tekemiselle, jossa otetaan huomioon, millä keinoilla tasoa pystytään jatkossa ylläpitämään sekä seuraamaan.

Perustaso käsittää tietoturvallisen käyttäytymismallin päivittäisessä työnteossa sekä organisaation omien käytänteitä työasemien käytössä sekä turvallisen verkossa käyttäytymisen.

Tämän hetkinen koulutus organisaatiossa pohjautuu ryhmäkeskusteluun organisaation käytänteistä, josta jää merkintä koulutusrekisteriin. Itse koulutukseen osallistutaan työsuhteen alkaessa tai jos siihen ei ole toistaiseksi jostain syystä päässyt osallistumaan eli koulutukseen osallistuvien kokemus organisaation sisäisistä turvallisuusmenetelmistä on vaihtelevaa. Koulutuksen jälkeen ei ole formaalia jatkokoulutusta tai seurantaa, joissa vastattaisiin kysymyksiin, onko kyseisiin menetelmiin sitouduttu tai onko menetelmissä kehittämisen varaa. Näihin kehityspisteisiin pyritään luomaan neutralisoivia keinoja, jotta koulutuksesta tulisi entistä strukturoidumpi sekä hallitumpi.

7.1 Perustaso

Oppaan tarkoituksena on luoda perustaso, jolla yksityiselämässä tai työympäristössä toimiva henkilö pystyisi toimimaan tietoturvallisemmin. Ajatuksena on luoda yleistä laatua oleva lähtötilanne työntekijälle, jotta organisaatiokohtaisia sekä tarkempia ohjeistuksia pystytään mahdollisesti jatkossa ymmärtämään. Oppaan tavoite on, että lukija implementoisi omaan käyttäytymiseensä turvallisia menetelmiä sekä vähintään ymmärtäisi, millaisia perusasioita tulisi ottaa huomioon tietoturvan käytännön toimien osalta. Dokumentaatiossa on kerätty muutamia tutkimuksia sekä uutisointeja lähimenneisyyden tapahtumista, joiden tavoitteena on perustella lukijalle, että asiat ovat ajankohtaisia.

Opas (Liite 13.) jaetaan kolmeen osaan Mitä, Miten ja Miksi, joka pohjautuu ISO 27002:2017 standardin määrittämään henkilöstöturvallisuuden hallintakeinoon

A.7.2.2, jonka mukaan tietoisuusohjelmassa olisi tärkeä keskittyä aikaisemmin mainittuihin kysymyksiin sekä niiden vastaamiseen koulutettavalle. Dokumentaatiossa on myös yksityiskohtaisempia ohjeistuksia salausmenetelmiin, koska tekninen taitotaso voi vaihdella lukijakunnittain.

Mitä-osiolla avataan aihealueen liittyvää sisältöä. Miten-osiossa kerrotaan kunkin aiheen käytännön osuus, eli millaisia turvalliseksi katsottuja menetelmiä ja keinoja teemaan liittyy. Miksi-osiossa kuvataan minkä takia teeman käsittelemän aihealueen turvallisuuteen tulisi kiinnittää huomiota. Lisäksi Miksi-osiossa on lueteltu kolme positiivista pointtia ja riskiä teemaan liittyen.

Oppaan teemat ovat seuraavanlaisia:

- Päivitykset
- Työasema ja laitteisto
- Tietojenkäsittely
- Verkkokäyttäytyminen
- Salalauseet

Tavoitteena perustasolla on, että lukija ymmärtää laitteistojen sekä ohjelmistojen päivityksen tärkeyden sekä ylläpitää laitteistojaan ajantasaisina sekä pystyisi itseohjautuvasti päivittämään käyttöjärjestelmän, selaimen sen laajennukset sekä tarkastamaan BIOS:n ajantasaisuuden.

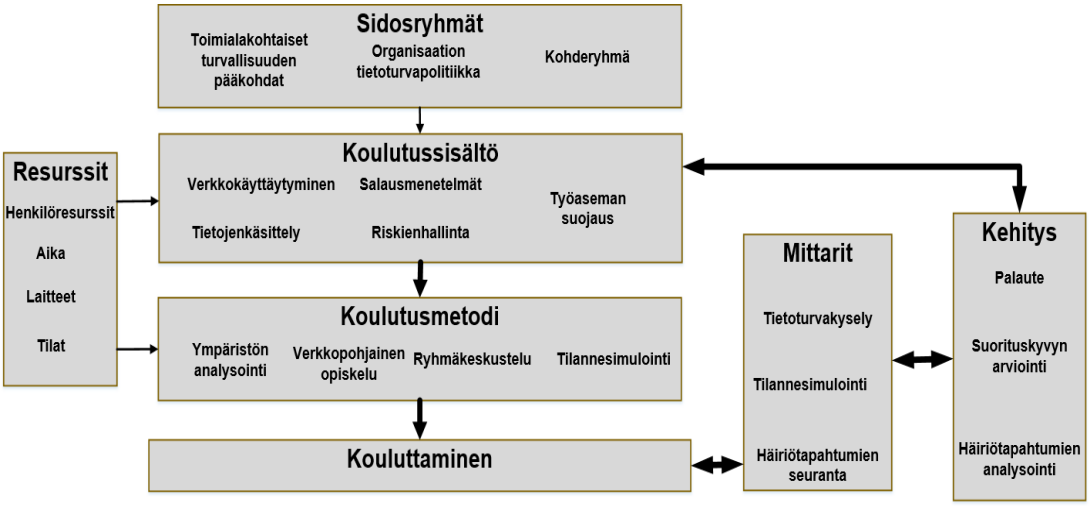
Ymmärtää käyttämiensä päätelaitteiden olevan haavoittuvaisia ja pystyy ylläpitämään laitteistojaan turvallisina omalla käyttäytymisellään sekä suojausmenetelmillä. Tietoisuus turvallisesta tietojenkäsittelystä sen elinkaaren aikana tulisi kasvaa sekä huomioida työnteossa.

Tavoitteena on, että lukija pystyisi tunnistamaan ja välttämään yleisimmät haittaohjelmien ilmenemismuodot sähköpostissa, internetissä sekä sosiaalisenmedian kautta. Sekä pystyy itseohjautuvasti seuraamaan tietovirtoja kyberturvallisuuteen liittyen sekä suojautumaan tarvittavilla toimenpiteillä varoituksien tai kyberuhkien ilmetessä.

Salalauseiden osalta tulisi ymmärtää mitä on turvallinen salalauseiden käsittely sekä pystyisi myös suojatusti käsittelemään tunnistautumistietojaan sekä pystyisi jatkossa tunnistamaan turvallisimmat kirjautumismenetelmät sekä käyttämään niitä.

7.2 Koulutuskehys

Organisaation asianmukaisen tietoturvakoulutukseen vaikuttaa monia tekijöitä, joita on kuvattu kuviossa 4. Opetussisällön ja metodin valinta on avainasemassa, kun tavoitteena on opastaa henkilöstöä toimimaan turvallisesti organisaatiossa. Kuviossa 4 olevassa mallissa on kuvattu koulutuskehys, jolla pyritään luomaan organisaation koulutusmetodiin vaikuttavia teemoja sekä askelia, joilla koulutusrakenne muodostuu sekä miten koulutuksen seuranta sekä kehitys vaikuttavat koulutuksen jatkuvaan kehitykseen. Kehykseen on otettu suuntaviivoja IJACSA (International Journal of Advanced Computer Science and Applications) julkaisusta, jossa käsiteltiin tehokkaan tietoturvallisuus koulutuksen luomista (Ghazvini & Shukur, 193-205).



Kuvio 4. Koulutuskehys

Sidosryhmillä tarkoitetaan koulutuksen kannalta merkittävästi opetussisällön luonteeseen sekä asiasisältöön vaikuttavia ryhmiä. Kyseisiin ryhmiin kuuluvat mm.

- Toimialakohtaiset tietoturvallisuuteen vaikuttavat pääkohdat
- Kohderyhmä
- Organisaation tietoturvapolitiikka

Toimialakohtaiset pääkohdat tietoturvallisuudesta käsittävät kyseisen kohdeorganisaation tapauksessa konsultointi sekä ohjelmistotalon asettamia vaatimuksia työnteon turvallisuudelle, kuten etätyöskentely, informaation käsittely, verkkokäyttäytyminen ja työasema turvallisuuteen liittyviä näkökulmia.

Pääkohtien löytämistä saattaa helpottaa yleisien tietoturvaongelmien havainnoinnilla, jolloin luodaan yleiskuva tämän hetkisistä uhkista ja riskeistä, jotka liittyvät kyberturvallisuuteen sekä työelämässä kuin yksityishenkilönä.

Kohdeorganisaation tapauksessa on kolme eri luokkaa konsultointi, hallinto sekä tuotekehitys, joissa työtehtävän mukaan työskennellään erilaisissa työympäristöissä, jotka asettavat erilaisia vaatimuksia tietoturvataitojen kehittämiseen.

Koulutuksen materiaalin sisältöön vaikuttaa organisaation työntekijöiden taitotaso, sekä rooli jolloin koulutuksen sisältö tulisi saattaa koulutettavien vaatiman tason mukaiseksi. Sisällön muokkaaminen kohdeyleisölle sopivaksi vähentää yli- ja alikouluttamisen vaara, jota tulisi karttaa, jotta koulutus ei muutu liian vaikeaksi tai helpoksi ymmärtää. Kuitenkaan unohtamatta, että pohjatieto tulisi kaikilla kohderyhmillä olla sama ja ylläpidetty.

Koulutuksen sisällön tulisi nojautua myös organisaation tietoturvapolitiikan asettamien näkökulmien mukaiseksi, jolloin organisaation tietoturvapolitiikan kautta asettamat tavoitteet voidaan sitouttaa koulutuksen sisältöön.

7.2.1 Koulutussisältö

Opetussisältö muodostuu sidosryhmien asettamien teemojen sekä tarpeiden ja tavoitteiden mukaan. Kohdeorganisaatiossa opetussisältöön voidaan kattaa perustasoa tukevoittaviin teemoihin, joissa käsitellään turvallista verkkokäyttäytymistä, tietojenkäsittelyä, salausmenetelmiä, työaseman suojausta, viestintää sekä vastuita organisaatiossa sekä riskienhallintaa.

Koulutuksessa käytävän sisällön tulisi vastata koulutettaville seuraaviin kysymyksiin:

- Mitä? Mitä asioita kyseiseen teemaan kuuluu sekä organisaation asettamat odotukset työntekijälle.
- Miten? Miten toimitaan kyseisen teeman rajoissa turvallisesti ja täytetään vaaditut odotukset.
- Miksi? Miksi kyseisen aihealueen asiat ovat organisaatiolle tärkeitä sekä miksi asioihin panostetaan. Koulutettavalle tulisi käydä selväksi myös millaisia riskejä kyseisestä turvallisuusmenetelmien rikkomisesta saattaa seurata.

7.2.2 Koulutusmetodi

Oikean opetusmetodin valintaan on pohdittava teemoittain sopivinta vaihtoehtoa, koska henkilöstölle sekä organisaation kulttuurille sopivin metodi tuo myös onnistumistasolla parhaimman ja todennäköisesti halutuimman lopputuloksen. Opetusmetodin valintaan kuin myös sisällöllisesti koulutukseen vaikuttaa siihen vaaditut resurssit, kuten raha, aika, tilat, henkilöresurssit sekä mahdolliset laitehankinnat.

Tutkimusvaiheessa kohdeorganisaation ollessa kehitysvaiheessa ja ns. pk-yrityksen tasolla, resurssien niukkuus on huomattavaa, joten on todennäköistä, että karsintaa tapahtuu opetusmetodin valinnassa riippuen organisaation tahtotilasta resursoida henkilöstön pätevöittämiseen. Ehdotettavia koulutusmetodeja voivat olla aivoriihet, verkkopohjainen opiskelu, ryhmäkeskustelut tai tilannesimuloinnit.

Eräs metodi kehittää koulutettavien tietoturvatietämystä on koota kyberturvallisuuteen liittyviä tapahtumia, joissa organisaatiossa on jouduttu hyökkäyksen tietovuodon, murtojen tai haittaohjelmien leviämisen kohteeksi ja käsitellä miten tilanne pystyttäisiin estämään olemassa olevilla työkaluilla tai miten omassa organisaatiossa pystyttäisiin palautumaan mahdollisesta ongelmatilanteesta. Metodi vaatii aikaa koulutustilaisuuteen vaaditun ajan sekä pohjamateriaalin valintaan vievän ajan, johon vastuuhenkilö tuottaa listausta tietoturvatapahtumista maailmalla.

Verkkopohjaisella opiskelulla koulutettavat saavat omatoimisesti opiskella organisaation käytänteitä niille varastusta palvelusta tai sitten omatoimisesti osallistumalla kolmannen osapuolen tarjoamaan tietoturvakoulutukseen. Koulutusmetodi ei vaadi keskitettyä koulutustilaisuutta, mutta resurssit keskittyvät organisaation sisäiseen tietopankkiin, jota tulee päivittää, johon tulee nimetä vastuuhenkilö. Tämän tyyppisen koulutusmetodin seurantaan on käytännöllistä käyttää kyselypohjaista seurantaa.

Ryhmäkeskusteluna toimiva koulutus pohjautuu normaaliin luokkatilaopetukseen, jossa käydään keskustelun tapaisesti turvallisuusasioita läpi, kuten kohdeorganisaatiossa on toimittu tähänkin mennessä. Keskustelun etuna on tarvittavien resurssien vähyys, tosin opetusmenetelmänä ei välttämättä palvele kaikkia osallistujia, johon tulee kiinnittää huomiota metodin käytön tehokkuuden mittauksessa.

Tilannesimuloinnilla voidaan harjoitella käytännön turvallisuusmenetelmiä ja näin laittaa osallistujat kädet saveen-tyyppiseen tilanteeseen. Usein tietoturvallisuuteen liittyykin juuri käytännön toimia henkilöstöltä, joten tapa palvelee hyvin työssä vastaantulevia tilanteita, ja tilannesimulointi voi hyvinkin toimia tietoisuuden seurantavälineenä koulutukselle.

7.3 Koulutusprosessi

Ennen varsinaista koulutusta pohjatyönä on suunnitella, mitä tavoitteita organisaatiolla on ja mitkä niistä ovat kriittisimpiä, joihin tulisi eniten panostaa. Opetussisällöllisesti on tärkeää määritellä kohderyhmän perusteella, mikä metodi sopii parhaiten, jolloin saataisiin tilanne, jossa mahdollisimman vähäisellä ajankäytöllä saadaan paras lopputulos. Lisäksi vastuuhenkilöiden sekä tarpeellisten resurssien määrittäminen koulutukselle sekä koulutuksen suorituskyvyn seuraamiseen liittyvistä asioista, kuten haluttu suorituskykymittari sekä miten viestitään tuloksista ja kenelle. (Best Practices for Implementing a Security Awareness Program 2014, 12.)

Ensimmäinen tasomittauksen avulla saadaan henkilöstön lähtötaso, johon voidaan soveltaa haluttua metodia, kuten tietoturvakyselyn tapaista kartoitusta, josta saadaan pohjatieto tulosten analysointiin jatkossa.

Ensimmäinen koulutus voidaan tehdä tavanomaisin menetelmin, eli ryhmäkeskusteluna, josta valitun ajanjakson kuluttua suoritetaan uusinta tasokokeesta, joka voidaan tehdä joko tilannesimulaatiolla tai tietoturvakyselyn mukaan. Seurannan tarkoituksena on mitata henkilöstön tietoisuudentason muutosta koulutettuun teemaan nähden sekä koulutuksen tehokkuutta.

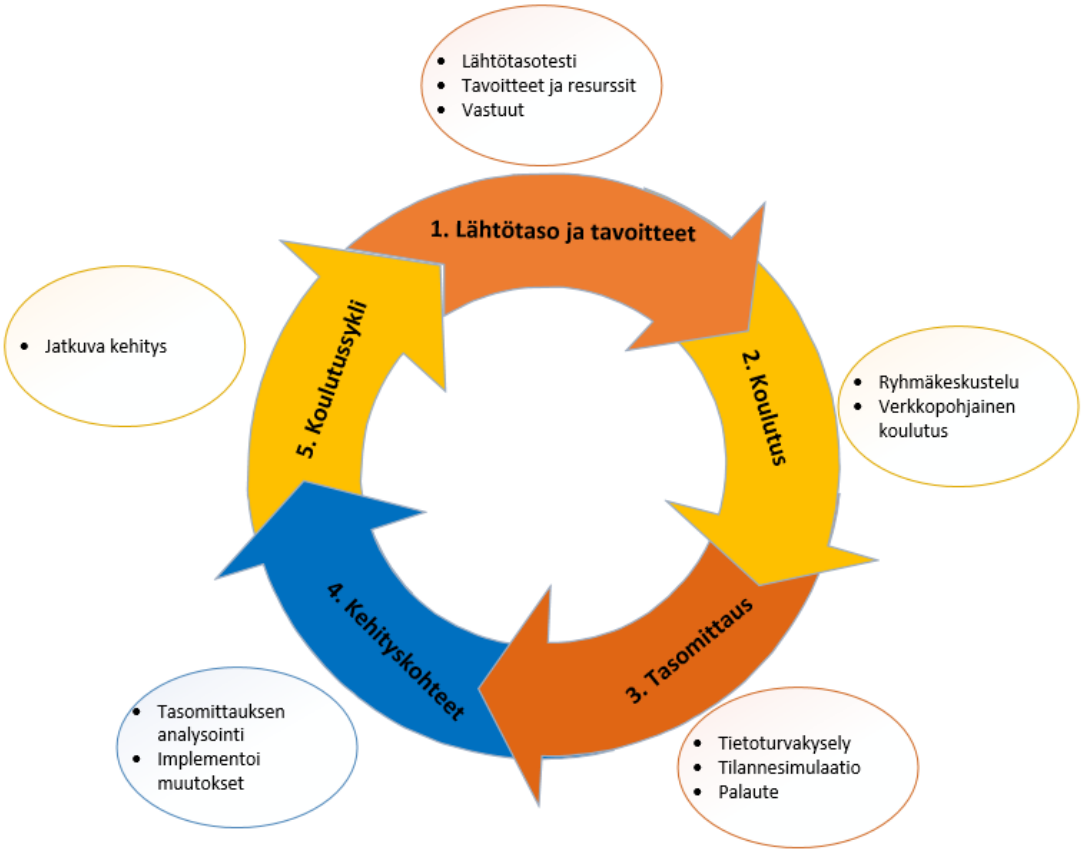
Tulosten analysoinnin pohjana tulisi olla tasomittausten tulokset eli henkilöstön lähtötaso sekä toisen tasomittauksen tulokset ja näiden tulosten peilaus asetettuihin ta-

voitteisiin. Huomioon otettavaa on myös koulutuksesta saatu palaute myös mahdollisia kehityskohteiden harkinnassa jatkokoulutusta ajatellen. Tärkeitä kysymyksiä, joihin tulisi hakea vastausta kehityksen osalta on mm.

- Millaisia vaikutuksia koulutuksella oli henkilöstön tietoturvalliseen käyttäytymiseen?
- Miten henkilöstö suhtautui koulutuksen haastavuuteen sekä toteutukseen?

Koulutuksen kehittäminen on ensisijaisen tärkeää, jotta hyötysuhdetta koulutukseen käytettyjen resurssien ja saatujen tulosten välillä saadaan nostettua. Kehitysvaiheen päätösten tulisi pohjautua koulutuksen suorituskyvyn arvioinnista saatuihin tuloksiin sekä myös henkilöstöltä saatuun palautteeseen. On myös oleellista katselmoida koulutukseen liittyviä tavoitteita sekä perustasoa, mahdollisia muutoksia varten, kuten asetettujen tavoitteiden saavuttaminen tai ympäristötekijöiden, kuten sidosryhmien vaatimusten tai teknologisten näkökulmien kehittyessä vaativimmiksi. Tällöin perustason sekä koulutussisällön päivittäminen ovat asialistalla.

Mahdollisten kehityskohteiden implementointi tulisi saattaa pikimmiten seuraaviin koulutustilaisuuksiin voimaantuleviksi, jolloin jatkuva kehitys voi tapahtua. Tällöin jokaisen tasomittauksen jälkeen voidaan kehittää organisaation koulutusmetodia sekä sisältöä toimintakulttuurin sekä haluttujen päämäärien mukaiseksi. Kuviossa 5 on esitetty koulutusprosessia. Teoreettisesti pohjana toimii PCI Data Security Standard:n julkaisu parhaista käytänteistä implementoida turvakoulutuksia (Best Practices for Implementing a Security Awareness Program 2014).



Kuvio 5. Koulutusprosessi

7.4 Seuranta ja resurssit

Organisaatiossa ei keskitettyjä lokienseurantaa tai keskitettyä käyttäjienhallintaa josta voisi tarkempaa käyttäjäkohtaista seurantaa tehdä, joten on turvauduttava käytännönläheisempään seurantaan, kuten kyselyihin sekä tilannesimulointiin ja kehityskeskusteluihin. Tulosten seurannan avulla saadaan jatkuvaa tietoa koulutuksen suorituskyvystä sekä tarpeesta muuttaa mahdollisesti koulutusmetodeja tai sisältöä.

7.4.1 Tietoturvakysely

Perustason seuraamiseen voidaan soveltaa kuukausittaista teemoittain vaihtuvaa kyselyä. Kyselyn toteutus voidaan tehdä ennen ja jälkeen koulutuksen, jotta saadaan selville, onko henkilöstön tietotaito teemaan nähden kasvanut. Aiheina voi toimia

työaseman suojausmenetelmät, verkkokäyttäytyminen, salausmenetelmät, haittaohjelmien torjunta tai turvallinen tietojenkäsittely. Kyselyn tulokset käydään läpi seuraavan koulutuksen tullessa. Taulukossa 9 on kuvattu tarkemmin millainen mahdollisen suorituskyvyn mittaamiseen käytettävän tietoturvakyselyn peruskuva voisi olla.

Taulukko 9. Tietoturvakysely

Työkalu	Google Forms, Sharepoint kysely.
Seurataan	A. Koulutettujen pätevyydentasoa aikaisemman tietoturvakoulutuksen aihealueeseen liittyvien kysymysten avulla. B. Onko koulutuksella ollut haluttuja vaikutuksia teoreettiseen osaamiseen.
Hyödyt	Kyselyn toteutusmenetelmä ei vaadi suurta resurssointia. Toistettavissa sekä teemoituksen myötä pystytään seuraamaan tietyn aihealueen teoria tason osaamista. Kyselyn avulla pystytään myös keräämään rakentavaa palautetta koulutusmenetelmästä ja sen mielekkyydestä.
Haitat	Kyselyn avulla saadaan karkea arvio siitä, miten hyvin koulutuksen teeman mukaiset asiat ovat iskostuneet henkilöstöön. Turvallisen käytöksen mittaaminen jää teoreettisen osaamisen tasolle.
Resurssit	Kyselyiden luontiin, ylläpitämiseen ja analysointiin vaadittu aika.

7.4.2 Tilannesimuloinnit

Tilannesimuloinnin ajatuksena on rekonstruoida oikeita turvallisuusuhkia, joiden tavoitteena on seurata henkilöstön toimintamallia sekä onko jokin tietty riskitekijä henkilöstön käytöksessä olemassa, johon tulisi kiinnittää huomiota ja vastaisuudessa vaikuttaa koulutuksella käyttäytymismalliin.

Kalasteluviesti kampanja organisaation sähköpostiin suoritetaan siten, että ulkopuolisen palvelun avulla luodaan organisaation henkilöstölle tekaistuja kalasteluviestejä,

joilla seurataan, kuinka moni henkilöstön jäsen avasi viestissä olevan linkin tai liitetiedoston. Kampanja voidaan toistaa halutulla aikavälillä ja mahdollisesti vaihtaa vaikeusastetta, kuinka helposti tunnistettavissa viesti on. Viestien teemoina voi olla:

- Kutsu kokoukseen, jossa lisämateriaali linkin takana
- Toimitusjohtajan tärkeä ilmoitus

Tärkeää on, että tulokset paljastetaan lähetetyn viestin kera henkilöstölle. Kampanjan tavoitteena ei ole listata kuka henkilöstöstä lankesi ansaan vaan kartoittaa, kuinka henkilöstö käyttäytyy tilanteessa ja näin ollen lisätä tietämystä aiheeseen liittyen, jos siihen on tarvetta. Taulukossa 10 on arvioitu kalasteluviesti kampanjan hyötyjä sekä haittoja.

Taulukko 10. Kalasteluviestikampanja

Työkalu	InfoSec Instituutin SecurityIQ työkalu tai oma sähköpostipalvelin.
Seurataan	A. Kuinka moni organisaation henkilöstöstä mm. avasi viestin tai viestissä olleen linkin. B. Kuinka moni ilmoitti kalasteluviestistä johonkin organisaation viestiväylään.
Hyödyt	Tulokset on helppo analysoida ja jatkossa seurata, jos kampanjoita tehdään sovituin aikavälein.
Haitat	Vaatii oman sähköpostipalvelimen tai ulkopuolisen palvelun ja sitä kautta sen opiskeluun ja ylläpitoon vaadittu aika.
Resurssit	Aikaresurssit kampanjan luomiseen sekä mahdollisesti ulkoinen palveluun sijoitettavat resurssit.

Keskustelutilanteiden luonti, jossa aiheena on luottamuksellisen tiedon suojaaminen. Tilanteessa henkilöstö jaetaan ryhmiin ja annetaan jokaiselle ryhmälle oma tilanne, johon liittyy luottamuksellisen tiedon väärinkäyttö, vuoto tai poisto. Mahdollisia aiheita:

- Työaseman varastaminen
- Asiakastiedon vuotaminen verkkoon
- Työtiloihin murtautuminen
- Organisaation työasemiin on tarttunut kiristyshaittaohjelma

Jokainen ryhmä esittelee oman näkemyksensä, kuinka tilanne oltaisiin pystytty estämään tai millä keinoin suojaudutaan uhkalta. Keskustelusta voidaan luoda pöytäkirja mahdollisista ratkaisuista, joihin voidaan palata jatkossa ja analysoida kuinka neutralisoida tilanne. Tarkoituksena on löytää keskustelun avulla näkökulmia, onko koulutuksen avulla herännyt uusia menetelmiä tieto-omaisuuksien suojaamiseen. Taulukossa 11 on esitetty ryhmäkeskustelutilanteen hyötyjä sekä haittoja.

Taulukko 11. Teemoitettu ryhmäkeskustelutilanne

Seurataan	A. Onko tietoisuus kasvanut, kuinka toimia hätä- tai uhkatilanteissa.
Hyödyt	Keskustelun kautta pystytään hakemaan uusia ajatuksia, miten tilanne neutralisoidaan tai miten tilanteessa tulisi kommunikoida työyhteisölle.
Haitat	Vaatii aikaa sekä motivaatiota osallistua toimintaan. Tulosten analysointi jää keskustelun tasolle eikä sinänsä luo mahdollista pöytäkirjaa kummempaa analysoitavaa tulosta.
Resurssit	Vaatii aikaa vastuuhenkilöltä dokumentoinnin ylläpitoon sekä uusien tapausten luontiin. Tilavaraukset.

Muistivälineiden käyttöön liittyen organisaatiossa voidaan toteuttaa muistiväline kampanja, jossa toimitiloihin asetetaan muistitikkuja, jotka toimivat ns. ”saastuttavina tikkuina”, joiden avulla seurataan kuinka tarkasti henkilöstö analysoi työasemiinsa kytkemiään muistivälineitä.

Muistivälineissä tulisi olla viesti, jonka kautta mahdollinen tikun käyttäjä ymmärtää laittaneensa päätelaitteeseensa tuntemattoman muistivälineen. Viestissä voi olla vaikkapa linkki, jossa muistivälineen käyttäjän tulisi käydä, jossa seurataan, kuinka

moni käytti muistitikkua. Halutun aikavälin jälkeen tehdään koonti, kuinka monta kertaa muistivälineitä käytettiin työasemissa. Taulukossa 12 on esitetty muistiväline kampanjan liittyen hyötyjä sekä haittoja kuin myös mitä asioita konkreettisesti pystytään seuraamaan.

Taulukko 12. Muistivälinekampanja

Työkalu	Haluttu määrää muistitikkuja sekä mahdollisesti seuranta linkki.
Seurataan	A. Kuinka moni muistitikku kytkettiin työasemaan B. Kuinka moni ilmoitti tuntemattomasta muistivälineestä
Hyödyt	Helppo ja näppärä tapa seurata henkilöstön toimintatapoja. muistivälineiden käytössä.
Haitat	Toimialan mukaan osa henkilöstöstä toimii asiakkaantiloissa, joten koskee organisaation toimitiloissa työskenteleviä. Seuranta aiheuttaa haasteita, koska perustuu luottamukseen, että henkilö oikeasti käy seurantalinkin takana.
Resurssit	Haluttu määrää muistitikkuja sekä niiden alustamiseen vaadittu aika.

Henkilöstön käyttäytymistapoja voidaan seurata myös teettämällä huijausviestejä, jonkin henkilöstön käyttäjätilin kautta, jolloin käytännössä valitaan yksi organisaation henkilöstöstä, jonka tulee toimittaa johonkin organisaation sisäiseen viestintäkanavaan yhden päivän aikana ”vihamielinen” linkki. Viestistä tulisi käydä ilmi merkkejä, joilla tunnistaa, että tili on kaapattu. Toteutustapa vaatii ennalta suunnittelua, kuka, milloin ja miten. Taulukossa 13 on esitetty murretun käyttäjätiliin vaadittuja resursseja sekä hyötyjä sekä haittoja.

Taulukko 13. Murrettu käyttäjätili

Työkalu	Organisaation viestintäkanavat sekä linkin seurantapalvelu, kuten Google URL-lyhennin.
Seurataan	A. Kuinka moni avasi ”kollegan” jakaman linkin. B. Kuinka nopeasti viestistä kommunikoidaan.
Hyödyt	Henkilöstön seuranta, kuinka arvioivat sisäisiin viestintäkanaviin tulleita ilmoituksia sekä viestejä. Halvasti suoritettavissa.
Haitat	Toteutustapa vaatii ennalta suunnittelua, kuka, milloin ja miten.
Resurssit	Viestinsuunnitteluun vaadittu aika sekä henkilöresurssit, kuka toimii viestin levittäjänä.

7.4.3 Häiriötapahtumien seuranta

Häiriötapahtumien seurannalla tarkoitetaan organisaatiossa tapahtuvien tietoturvahäiriöiden seurantaa, joissa henkilöstö on tarvinnut. Luodaan listaa, minkä laatuisia häiriöitä tai ongelmia henkilöstöllä on ollut, kuten työasemaan tarttuneiden haittaohjelmien määrä, henkilöstön avuntarve turvallisten menettelyjen suorittamisessa sekä laitteisto-ongelmat. Seurantaan liittyy häiriön kriittisyyden arviointi sekä luonteenlaadun arviointi. Taulukossa 14 on kuvattu häiriötapahtumien seurantaan liittyviä hyötyjä ja haittoja.

Taulukko 14. Häiriötapahtumien seuranta

Työkalu	Taulukointi- tai seurantaohjelma.
Seurataan	Organisaation henkilöstön A. Henkilöstön kypsyystasoa ratkaista ongelmia B. Viestintäkykyjä C. Aiheuttaako, jokin tietty palvelu tai toimintaongelmia
Hyödyt	Analysoimalla organisaatiossa tapahtuvia häiriötekijöitä ja ongelmatekijöitä saadaan hyödyllistä seurattavaa, myös pitemmällä aikavälillä, jos organisaatiossa laajennetaan käyttäjienhallinnallisia ominaisuuksia. Seurantaa voidaan kehittää jatkossa tapahtumien hallinnan tehokkuuden seuraamiseen esimerkiksi tietyssä aikavälissä ratkaistujen ongelmien määrään.
Haitat	Kaikkiin organisaatiossa ilmeneviin ongelmiin ei välttämättä koulutuksen kautta saada ratkaisua. Vaatii henkilö resurssointia seurannan mahdollistamiseksi.
Resurssit	Vastuuhenkilöltä vaadittua aikaa valitun dokumentointi menetelmän ylläpitoon.

8 Johtopäätökset

Tarkoituksen oli tutkia, millaiset valmiudet kohdeorganisaatiossa on tarkasteltavan standardin osalta omassa toiminnassaan noudattaa kyseistä viitekehystä. Asetettujen tutkimuskysymysten perusteella työntekijät arvostavat eniten asiakkaan informaatiota, jota mahdollisesti käsittelevät sekä yrityksen sisäisiä laiteresursseja, myös tuotekehityksen osalta käsiteltävän tuotteen myötä ohjelmistollisia resursseja.

Tutkimukseen viitekehyksenä toiminut standardin ydinideana on riskienhallinta, johon kuuluu omat vaiheensa turvallisuuden jatkuvaan kehitykseen. Tällöin viitekehyksen mukainen toiminta on toistaiseksi suunniteltavuuden sekä kehityksen osalta määrittelemätöntä ja sisältää suuria kehityskohteita, kuten sidosryhmien tarpeiden ja vaatimusten analysointi sekä niiden tuominen riskienhallinta toiminnan tietoturvalli-

suuden kehitykseen. Esille tuli myös käytännön hallintakeinojen vajavaista toteuttamista sekä epäjärjestelmällisyyttä, mikä voi johtua resurssien puutteesta tai henkilöstön tietoturvallisen toiminnan kehitystarpeesta. Toiminnallisesti suorituskyvyn arviointi sekä parantaminen on ollut vähäistä sekä hyvin pitkälti yksittäisten arviointien sekä kehitystoimien pohjalla, eli vähäisellä suunniteltavuudella ja toiminnan kehitykseen liittyvää arviointia.

Tutkimuskohteena olleen organisaation käytössä olevilla resursseilla on hankala täyttää jokaista puutoskohtaa, kuitenkin toimintaympäristön analysoinnilla saadaan kuvaa mitä tietoturvallisen toiminnan tavoitteita organisaatio tavoittelee oman toiminnan kehityksessään sekä tietoturvallisessa toiminnassaan.

Riskienhallinnallisesti tietoturvariskien käsittelyyn sekä arviointiin tulisi saattaa lisää resursseja ja löytää toimintaan hyvä struktuuri sekä hallintamenetelmien kehitys.

Katsottiin, että kehityskohteeksi on järkevä valita koulutusmenetelmien kehitys sekä luoda näin ollen pohjataso ehdotus organisaatioon, jota ylläpitää. Tunnistettiin, että koulutus on ilman sen suurempaa struktuuria, joten hyvien käytänteiden kehittämisessä tietoturvakoulutuksen osa-alueella pystytään kehittämään henkilöstöturvallisuutta sekä vähentämään inhimillisten virheiden riskiä.

9 Pohdinta

Aihe oli kiinnostava, koulutusalaan nähden tietotaito pohja aiheelle oli kuitenkin alustavasti vähäinen ja tutkimus teettikin lisätyötä, kuinka hankkia tietoa organisaation toiminnasta, miten muokata sekä käsitellä saatua informaatiota sekä mikä on tutkimuksen kannalta olennaista tietoa. Tutkimus oli siinä mielessä haastava, että aihealueen ollessa riskienhallinta standardi kuten ISO 27001 on tutkimusalue laaja, joten tulee pohtia, mikä määrä kerättyä informaatiota on riittävä käsiteltäväksi.

Tällöin tarkka prosessipohjainen käsittely on jäänyt tästä tutkimuksesta vähemmällä, vaikkakin ilmi tulleiden asioiden pohjalta kohdeorganisaatiossa ei toistaiseksi ollut prosessimaista toimintaa kovinkaan paljoa. Tutkimusmenetelmällisesti suunnitelmallisuuteen vaaditaan enemmän panoksia, jotta tutkimuksen selkeät tavoitteet voisivat

olla yksityiskohtaisempia sekä metodologia sekä analyysimenetelmien perustelut tulisivat selkeästi esille.

Tavoitteena oli luoda nykytilan kartoitus kohdeorganisaatioon ja tehdä löydetyn epäkohdan kehitysehdotus, jossa onnistuttiin yleisellä tasolla. Yksityiskohtaisempi tarkastelu kohdeorganisaation tietoturvantilanteeseen jäi hieman vajavaiseksi, tutkimusmenetelmällisistä syistä.

Kartoitus on yleisellä tasolla suoritettu tarkastelu tilanteesta eikä välttämättä tarjoa niin paljoa kipupisteitä, kuin tarkempi tarkastelu olisi mahdollisesti tuonut. Työn lähtökohtiin nähden aikaansaannokset olivat tavoitteen mukaisia, vaikkakin tavoitteiden suunniteltavuus olikin ajoin haasteellista, mitä työltä halutaan. Tarkempi tavoitteiden suunniteltavuus ja päämäärä olisivatkin tärkeitä kehityskohteita tutkimusmenetelmällisesti määrittää selkeämmin paremman lopputuloksen saamiseksi.

Pk-yrityksen näkökulmasta kyseinen viitekehys on tietyiltä osin ylilyönti noudattaa, olemassa olevien resurssien puitteissa ja vaatii tarkempaa soveltamisen taitoa, mitkä ovat juuri kohdeorganisaation tarpeiden näkökulmista oikeat osa-alueet, jota lähteä soveltamaan omaan työympäristöön.

Mielenkiintoista olisi jatkotutkimuksena yleinen toimiala tarkastelu, mitä asioita standardista kohdeorganisaation toimialalla olevat Pk-organisaatiot ovat implementoineet toimintaansa ja kuinka paljon kyseistä viitekehystä käytetään toimialalla ja millaisia hyötyjä he ovat niistä saaneet.

Lähteet

Best Practices for Implementing a Security Awareness Program. 2014. PCI Security Standards verkkosivut. Viitattu 26.2. 2018. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Calder, A. & Watkins, S.2006. International IT Governance An Executive Guide To ISO17799 / ISO 27001. Lontoo: Kogan Page.

Curtis. P, & Carey. M, 2012. Risk Assessment in Practise. Viitattu 1.3.2018. https://www.coso.org/Documents/COSO-ERM-Risk-Assessment-in-Practice-Thought-Paper-October-2012.pdf.

GDPR Key Changes. N.d. Artikkeli EUGDPR-sivustolta. Viitattu. 17.1.2018. https://www.eugdpr.org/key-changes.html

Ghazvini, A. & Shukur, Z. 2017. Framework for an Effective Information Security Awareness Program in Healthcare. International Journal of Advanced Computer Science and Applications, 8, 2, 193-205. Viitattu 13.2.2018. http://thesai.org/Publications/ViewIssue?volume=8&issue=2&code=IJACSA

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Viitattu 15.11.2017.

Haruki, E. 2017. The CIA Triad of Information Security. RSI-Security Blog verkkosivut. Viitattu 12.11.2017. https://info.rsisecurity.com/blog/the-cia-triad-of-information-security

Horizon scan report. 2017. BSI:n verkkosivut. Viitattu 13.2.2018. https://www.bsigroup.com/LocalFiles/en-CA/press-release-material-2017/BSI-IS-ISO-27001-BCI-Horizon-Scan-Business-Continuity-CA-EN.pdf

Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 17.1.2018. https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Kosutic, D. N.d.a. The basic logic of ISO 27001: How does information security work?. Viitattu 3.4.2018. https://advisera.com/27001academy/knowledgebase/the-basic-logic-of-iso-27001-how-does-information-security-work/

Kosutic, D. N.d.b. Explanation of ISO 27001:2013 clause 4.1 Understanding the organization. 27001 Academy verkkosivut. Viitattu 18.11.2017. https://advisera.com/27001academy/knowledgebase/explanation-iso-270012013-clause-4-1-understanding-organization/?icn=free-knowledgebase-27001&ici=top-explanation-of-iso-27001-2013-clause-4-1-understanding-the-organization-txt

Kosutic, D. N.d.c. ISO 27001:2013 Foundations Course. Advisera eTraining verkkokurssi. Viitattu 1.12.2017. https://training.advisera.com/.

Kosutic, D. N.d.d. ISO 27001 vs. ISO 27002. 27001 Academy verkkosivut. https://advisera.com/27001academy/knowledgebase/iso-27001-vs-iso-27002/

Kosutic, D. 2016. What is an Information Security Management System (ISMS) according to ISO 27001?. 27001 Academy verkkosivut. Viitattu 18.11.2017. https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/

Riskienhallinta: kehittämistoimenpiteet. N.d. Pk-yrityksen riskienhallinta verkkosivut. Viitattu 26.11.2017. http://virtual.vtt.fi/virtual/pkrh/tyovalineet/haavoittuvuusanalyysi-1/riskien-hallinta-kehittamistoimenpiteet.html.

Riskienhallinta Mistä riskienhallinnassa on kysymys. N.d. Suomen Riskienhallintayhdistys PK-RH-riskienhallinta verkkosivut. Viitattu 26.11.2017. https://www.pk-rh.fi/riskienhallinta.html

Riskien luokittelu ja riskiesimerkkejä. N.d. Riskikompassin verkkosivut. Päivitetty 18.12.2017. Viitattu 26.2.2018. https://riskikompassi.fi/riskien-luokittelu

SFS-EN ISO/IEC 27000:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 12.11.2017. https://janet.finna.fi/Record/janet.318786. SFS Online.

SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat.Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 12.11.2017. https://janet.finna.fi/Record/janet.318786. SFS Online.

SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 3.3.2017. Viitattu 14.11.2017. https://janet.finna.fi/Record/janet.318786. SFS Online.

SFS-EN ISO/IEC 27003:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 15.8.2011. Viitattu 15.11.2017. https://janet.finna.fi/Record/janet.318786. SFS Online.

Taleb, N. 2007. Musta Joutsen Erittäin epätodennäköisen vaikutus. Helsinki: Hakapaino.

Tuotantoverkon tutkimus ja kehitys. 2017. Toimeksiantajan sisäinen tutkimus. Viitattu 15.1.2018.

VAHTI-toiminnan organisointi. N.d. Viitattu 15.12.2017.http://vm.fi/vahti-toiminnan-organisointi.

VAHTI 5/2004. 2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen.Päivitetty 8.10.2009. Viitattu. 13.2.2018. https://www.vahtiohje.fi/web/guest/5/2004-valtionhallinnon-keskeisten-tietojarjestelmien-turvaaminen

VAHTI 3/2007. 2007. Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 3.4.2018.

https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229

VAHTI 22/2017. 2017. Ohje riskienhallintaan. Viitattu 28.2.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/80013.

Vogel, D. 2017. What is the Best Security Framework for your Business?. Viitattu 3.4. 2018. https://misti.com/infosec-insider/what-is-the-best-security-framework-for-your-business

Liitteet

Liite 1. Haastattelupohja

1. Kuvaile vastuualueesi työympäristössä?

2. Millä tavoin tietoturvallisuus koskettaa työskentelyäsi?

3. Määrittele työnkuvasi mukainen salainen tieto?

4. Millaisia tietoturvariskejä olet huomannut toimintaympäristössäsi?

5. Millaisiin asioihin kiinnittäisit enemmän huomiota toimintaympäristön tietoturvallisuuden kehittämiseksi?

6. Millaisia ajatuksia sinulla on nykyisistä työssäsi käytössä olevista tietoturvakäytänteistä?

7. Millä tavoin tietoturvahäiriöitä käsitellään toimintaympäristössä?

8. Miten järjestelmien pääsynhallinta on toteutettu?

9. Millä tavoin lähdekoodia suojataan?

10. Millä tavoin varmistat tietoturvallisuuden työskennellessäsi etätyöpaikalla?

11. Kerro millä tavoin suojaat/suojaisit yritykselle tärkeitä resursseja?

12. Millä tavoin suojaat salasanasi ja tunnistautumistietosi?

13. Kerro kuinka suojaat työasemalla (näyttö, työpöydällä olevat dokumentit) käsiteltäviä mahdollisesti salassa pidettäviä tietoja jos et ole paikalla?

14. Millä tavoin tietojärjestelmien teknisiä haavoittuvuuksia hallitaan?

15. Minkälaisia menetelmiä käytetään kehitysprosessien turvallisuuden takaamiseksi?

16. Millä keinoin testiaineistoja suojataan?

17. Kuinka viestit työyhteisössä tapahtuvista tietoturvatapahtumista?

Liite 2. Haastattelu A (salainen)

Liite 3. Haastattelu B (salainen)

Liite 4. Haastattelu C (salainen)

Liite 5. Haastattelu D (salainen)

Liite 6. Haastattelu E (salainen)

Liite 7. Haastattelu F (salainen)

Liite 8. Haastattelu G (salainen)

Liite 9. Haastattelu H (salainen)

Liite 10. Haastattelu I (salainen)

Liite 11. Haastattelu J (salainen)

Liite 12. Haastattelu K (salainen)

Liite 13. Opas

Pohjustus

Oppaan tarkoituksena on luoda perustaso, jolla yksityiselämässä tai työympäristössä toimiva henkilö pystyisi toimimaan tietoturvallisemmin. Ajatuksena on luoda yleislaatua oleva lähtötilanne työntekijälle, jotta organisaatiokohtaisia sekä tarkempia ohjeistuksia pystytään mahdollisesti ymmärtämään. Oppaan tavoite on, että lukija implementoisi omaan käyttäytymiseensä turvallisia menetelmiä sekä vähintään ymmärtäisi, millaisia perusasioita tulisi ottaa huomioon tietoturvan käytännön toimien osalta. Dokumentaatiossa on kerätty muutamia tutkimuksia sekä uutisointeja lähimenneisyyden tapahtumista, joiden tavoitteena on perustella, että asiat ovat ajankohtaisia.

Opas jaetaan kolmeen osaan Mitä, Miten ja Miksi, joka pohjautuu ISO 27001:2017 standardin määrittämään henkilöstöturvallisuuden hallintakeinoon A.7.2.2, jonka mukaan tietoisuusohjelmassa olisi tärkeä keskittyä aikaisemmin mainittuihin kysymyksiin sekä niiden vastaamiseen koulutettavalle. Dokumentin lopussa on myös päivittämiseen sekä salausmenetelmiin laadittuja ohjeita.

Mitä-osiolla avataan aihealueen liittyvää sisältöä. Miten-osiossa kerrotaan kunkin aiheen käytännön osuus, eli millaisia turvalliseksi katsottuja menetelmiä ja keinoja teemaan liittyy. Miksi-osiossa kuvataan minkä takia teeman käsittelemän aihealueen turvallisuuteen tulisi kiinnittää huomiota. Lisäksi Miksi-osiossa on lueteltu kolme positiivista pointtia ja riskiä teemaan liittyen.

Ohjeistuksessa käydään läpi yleisien tietoturvaongelmien ratkaisuja sekä tarjotaan yksityiskohtaisempia ohjeistuksia järjestelmän päivitykseen sekä salausmenetelmiin. Ohjeistus on osioitu seuraavanlaisesti:

- Päivitykset
- Työasema ja laitteisto
- Tietojenkäsittely
- Verkkokäyttäytyminen
- Salalauseet

Dokumentaatiossa käytettävä ✓ merkintä kertoo aihealueeseen liittyvän vinkin tai neuvon.

Tavoitteet

Ymmärtää laitteistojen sekä ohjelmistojen päivityksen tärkeyden sekä ylläpitää laitteistojaan ajantasaisina sekä pystyisi itseohjautuvasti päivittämään käyttöjärjestelmän, selaimen sen laajennukset sekä tarkastamaan BIOS:n ajantasaisuuden.

Ymmärtää käyttämiensä päätelaitteiden olevan haavoittuvaisia ja pystyy ylläpitämään laitteistojaan turvallisina omalla käyttäytymisellään sekä suojausmenetelmillä. Tietoisuus turvallisesta tietojenkäsittelystä sen elinkaaren aikana tulisi kasvaa sekä huomioida työnteossa.

Pystyy tunnistamaan ja välttämään yleisimmät haittaohjelmien ilmenemismuodot sähköpostissa, internetissä sekä sosiaalisenmedian kautta. Pystyy itseohjautuvasti seuraamaan tietovirtoja kyberturvallisuuteen liittyen sekä suojautumaan tarvittavilla toimenpiteillä varoituksien tai kyberuhkien ilmetessä.

Salalauseiden osalta tulisi ymmärtää mitä on turvallinen salalauseiden käsittely sekä pystyisi myös suojatusti käsittelemään tunnistautumistietojaan sekä pystyisi jatkossa tunnistamaan turvallisimmat kirjautumismenetelmät sekä käyttämään niitä.

Sisällys

Mitä?

Päivitykset

Käyttämiisi laitteistoihin, käyttöjärjestelmiin sekä ohjelmistoihin tarjotaan jatkuvasti päivityksiä, jotka korjaavat löydettyjä haavoittuvuuksia sekä tietoturva-aukkoja. Tosiasia on, että monet haittaohjelmat käyttävät hyväksi käyttöjärjestelmästä sekä ohjelmistoista löytyviä haavoittuvuuksia. Mikään ohjelmisto, jota käytät ei ole täydellinen, mutta on lukijan etu huolehtia tarpeellisten ohjelmisto- ja käyttöjärjestelmäpäivitysten lataamisesta.

Laitteistoja ja ohjelmistoja, joiden ajantasaisuudesta tulisi huolehtia ovat mm.

- Käyttöjärjestelmä
- Selaimen lisäosat
- Ohjelmistot ja erityisesti tietoturvaohjelmisto
- Verkkolaitteet
- Älypuhelin
- Iot-laitteet

Verkossa rikolliset etsivät päivittämättömiä laitteita, ja käyttävät niitä hyväkseen. Huonoimmassa tapauksessa rikollinen pystyy ujuttamaan haittaohjelman syvälle organisaation järjestelmiin ja tätä ei huomata ollenkaan.

F-Securen tekemän tutkimuksen mukaan vanhojen haavoittuvien Android-versioiden käyttö on vielä yleistä, mikä on huolestuttavaa, koska samaisessa tutkimuksessa todettiin, että 99% mobiililaitteille suunnatuista haittaohjelmista on suunniteltu Android-laitteille.

Esineiden Internetissä piilee muitakin tietoturvaongelmia kuin vain päivittämättömyys, kuten salasanojen sekä suojaamattomien yhteyksien käyttö, mutta ensisijaisesti laitteistolle tarjottujen turvapäivitysten ajaminen olisi pääprioriteetti.

Työaseman suojaus

Tee ajatusleikki ja kuvittelet mitä henkilökohtaista tai yritykselle tärkeitä tietoja et halua jakaa muille henkilöille tai kolmansille osapuolille.

Työskennellessäsi päätelaitteellasi käsittelet paljonkin erilaista materiaalia, kuten vaikkapa, kuvia, videoita, tiedostoja, yhteystietoja, asiakirjoja, asiakastietoja tai työpaikkasi sisäistä materiaalia.

Kaiken tämän pitäminen luottamuksellisena ja saatavilla vain tietyille tahoille on hyvin pitkälti työaseman suojausmekanismien sekä viime kädessä **käyttäjän omien toimien harteilla.**

Päätelaitteiden suojaamiseen liittyy ainakin seuraavia näkökulmia

- Työaseman käytönvalvonta
- Pääkäyttäjätunnukset
- Salausmenetelmät
- Turvaohjelmisto
- Turvallinen tietojenkäsittely
- Päivitykset

Se millä tasolla päätelaitteesi tietoturvallisuus on, riippuu paljolti, miten olet varautunut tietomurtoon, laiterikkoihin sekä kuinka käyttäydyt verkossa ja miten olet panostanut turvallisuuden toteutumiseen päivittäisessä työnteossa ja vapaa-ajalla.

Tietojenkäsittely

Tietoa käsitellään nykyään kahdessa eri muodossa fyysisinä asiakirjoina sekä elektronisesti datana muistivälineillä sekä verkossa. Molempien käyttötapojen mukana tulee omat menetelmänsä, kuinka tietoa tulisi turvallisesti

- Säilyttää
- Siirtää/Käsitellä/Jakaa
- Hävittää

Jotta tietoja pystytään suojaamaan niiden elinkaaren aikana, tulee ensin määrittää, mikä on sellaista informaatioita, jota tulisi suojella.

- Organisaatioissa on yleensä tehty riskikartoitusta, jonka pohjalta on löydetty suojattavia resursseja, joiden turvallisuuteen tulisi panostaa hallintakeinoja sekä menetelmiä.

- Yksityishenkilönä on pohdittava, mitä tietoja ulkopuolisia saattaisi kiinnostaa. Sellaisia voivat olla esimerkiksi paikkatiedot, henkilötiedot, kontakti- ja viestintätiedot, pankkitiedot, kuvat, tiedostot, työmateriaali, käyttäjätunnukset ja salasanat.

Verkkokäyttäytyminen

Se miten päätelaitteen käyttäjä ymmärtää ja tiedostaa Internetissä piileviä riskejä sekä osaa välttää niitä, on avainasemassa turvallisen työskentelyyn sekä vapaa-ajan viettoon verkossa. Voidaan todeta, että ihminen ja sen valinnat ovat tärkein rajapinta tietoturvallisuuden ja tietomurron välillä.

Verkossa piilee ainakin seuraavanlaisia riskitekijöitä:

- Sähköposti
  - Huijausviestit
  - Tietojenkalastelu
  - Haitalliset liitetiedostot
  - Väärennetty lähettäjä
- Haittaohjelmien leviäminen
  - Virukset, troijalaiset ja madot
  - Kryptovaluutanlouhijat
  - Kiristysohjelmat
  - Palvelunestohyökkäykset
- Epäilyttävät tai väärennetyt verkkosivut
- Sosiaalisen media
  - Haitallisten linkkien avaaminen
  - Väärennetyt profiilit
  - Identiteettivarkaus
  - Yksityisyys
- Mobiililaitteiden käyttö
  - Julkisten verkkojen riskit

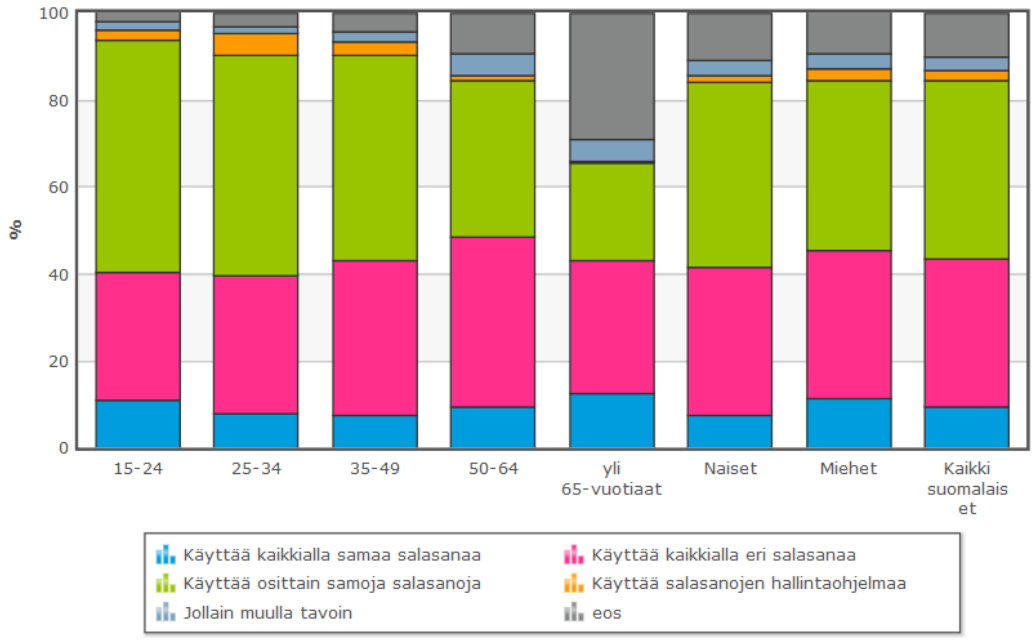
- Huijausviestit sekä puhelut
- Laitteen varastaminen

Pohdi itse millaisia epäilyttäviä asioita olet mahdollisesti havainnoinut verkossa pyöriessäsi ja miten olet estänyt tietojesi tai päätelaitteesi vaarantumisen.

Salalauseet

Liian helpot sekä ennalta arvattavat salasanat ovat ensimmäinen ja helpoin kompastus kivi, johon tavan käyttäjä saattaa tehdä virheen. Yleisimmin laiska käyttäjä sortuu kierrättämään samoja jo käytettyjä salasanoja tai jättävät epähuomiossa vaihtamatta, vaikkapa oletusasetuksilla olevan modeemin, älypuhelimen tai IoT-laitteen hallintapaneeliin tarvittavan tunnuksen salasanan. Erityisesti IoT-laitteiden kanssa tämä on yksi kehityskohde tietoturvan parantamiseksi.

Viestintäviraston kuluttajatutkimuksen mukaan erityisesti saman tai osittain saman salasanan uudelleenkäyttö on valitettavan suosittua. Alla kuviossa tutkimuksen tuloksia.



Viestintäviraston kuluttajatutkimuksen tuloksia (Lähde: https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2017/nettipuhelujenkayttoyleistynytvoimakkaasti.html)

On kuitenkin ymmärrettävä, että tänä päivänä salasanan murtaminen käy silmänräpäyksessä, jos et käytä riittävän turvallista salasanaa tai salalausetta. Voit testata verkosta löytyvillä palveluilla, kuinka nopeasti salasana murtuu.

Yleisradion artikkelin salasanakone.

Yleisimpiä oletussalasanoja tai huonoja salasanoja voit käydä tutkimassa mikrobitin artikkelista:

Miten?

Päivitykset

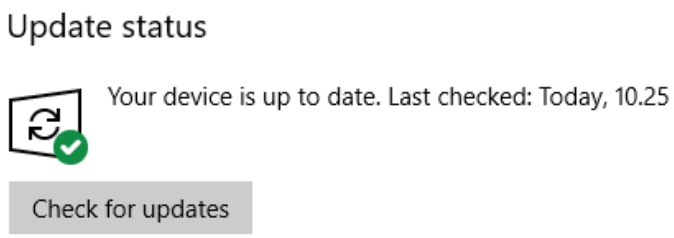
Seuraamalla viestintäviraston kyberturvallisuusvaroituksia pysyt ajan tasalla korjaavista laitteisto sekä ohjelmisto päivityksistä.

Huom työntekijä! Ennen uusien päivitysten asentamista varmista organisaatiossasi IT-tuelta onko luvanvaraista asentaa mahdolliset päivitykset. Isot versionostot saattavat aiheuttaa ongelmia käyttöjärjestelmän toiminnassa.

Käyttöjärjestelmä

Yleisimmin käyttöjärjestelmän päivitykset ovat asetettu automaattiseksi, kuten Windows 10-käyttöjärjestelmäss. Päivitysten ajoittainen tarkastaminen on kuitenkin suotavaa, varsinkin jos et ole käyttänyt työasemaasi hetkeen:

Asetukset -> **Päivittäminen ja suojaus** -> **Windows Update** -> **Tarkista päivitykset**



Käyttöjärjestelmän päivitysten kriittisyys

Päivitysten kriittisyys on otettava huomioon yksityiskäyttäjänä, sekä työntekijänä organisaatiossa. Käyttäjän tulisi itse huomioida, miten suuri vaikutus asentamattomalla päivityksellä saattaa olla, jos haavoittuvuuden hyväksikäyttö osuukin kohdalle. Esimerkkinä alla kuviossa Microsoft tarjoaa Windows-käyttöjärjestelmien turvapäivitysten yhteydessä vaikuttavuuden arvioinnin, josta käy ilmi kuinka suuri on pahin teoreettinen lopputulos, jos korjaavaa päivitystä ei ajeta ja haavoittuvuutta käytetään hyväksi.

Rating	Definition
Critical	A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs ***without*** warnings or prompts. This could mean browsing to a web page or opening email. Microsoft recommends that customers apply Critical updates immediately.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where client is compromised ***with*** warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered. Microsoft recommends that customers apply Important updates at the earliest opportunity.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. Microsoft recommends that customers consider applying the security update.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component. Microsoft recommends that customers evaluate whether to apply the security update to the affected systems.

Windows käyttöjärjestelmien turvapäivitysten vaikuttavuus luokittelu. (Lähde: https://technet.microsoft.com/en-us/security/gg309177.aspx)

Löydettyjen päivitysten KB-artikkelinumeron avulla pystyt hakemaan suojapäivitysoppaasta vaikuttavuus arvion.

Esimerkkinä alla Office-päivityksen korjaaman haavoittuvuuden hyväksikäyttöllä hyökkääjä pystyy ajamaan komentoja käyttäjän järjestelmään.

Date ▼	Product	Platform	Article	Download	Severity	Impact	Details
01/19/2018	Microsoft Office Compatibility Pack Service Pack 3		4011607	Security Update	Important	Remote Code Execution	CVE-20

Päivityksen lisätiedot päivitysoppaasta

Selain

Selain on yhtä lailla haavoittuvuuksien alainen. Siksi automaattinen päivitysten asetus on suotavaa. Pääset tarkastamaan selaimesi päivitysten tilan eri selaimissa:

Tarkista selaimesi ajantasaisuus

Google Chrome-selaimessa paina **Lisää-painiketta -> Ohje -> Tietoja Google Chromesta**

Firefox-selaimessa paina **Valikko-painiketta -> Ohje -> Tietoja Firefoxista**

Selaimen lisäosat

Tänä päivänä on yleistä, että käyttämääsi selaimeen lisätään erilaisia toiminnallisuuksia eli lisäosia. Lisäosiin pätevät samat lainalaisuudet kuten selaimen päivitykseen, eli aseta automaattiset päivitykset voimaan. Osa verkkosivuista käyttävät selainliittännäisiä erilaisten ominaisuuksien toimimiseen, kuten videoiden tai median katseluun.

Tällaisia liitännäisiä ovat mm. Adobe Flash Player, Oracle Java, Silverlight. Varsinkin Flash Player sekä Java ovat haavoittuvaisia, joiden käyttöä tulisi rajata vain kun se on tarpeellista ja muuten pitää käyttämättömänä.

Firefox-selaimella pystyt määrittämään automaattiset päivitykset lisäosiin valikosta:

Valikko-painike -> Lisäosat -> Valitse lisää tietoja -> Automaattiset päivitykset

Chrome-selaimella pystyt päivittämään laajennuksia valikosta:

Valikko-painike -> Lisää työkaluja -> Laajennukset -> Kehittäjätila -> Päivitä laajennukset nyt

Erilaisia lisäosia, jota asennetaan selaimeen tulisi myös arvioida luotettavuuden sekä tarpeen kautta. Lue lisäosan arvosteluja yleiskuvan saamiseksi, jotta tiedät mitä oikeuksia annat lisäosalle, jos asennat sen.

Alla listaus lisäosista, joista saattaa olla hyötyä:

uBlock Origin: Mainosten estäjä ja sisällönsuodattaja, joka lisää suodatinsääntöjä selaimeen, jotta erilaiset verkkosivujen elementit estetään, kuten mainokset ja pop-up sivut.

Firefox, Chrome

Flashblock: Haavoittuvan Flash-tekniikkan estämiseen verkkosivuilla käytetty lisäosa.

Firefox, Chrome

Disable WebRTC: Estää IP-osoitteesi näkyvyyden VPN-yhteyksien yli.

Firefox, Chrome

HTTPS Everywhere: HTTPS-protokolla suojaa verkkoyhteytesi Internetissä. Lisäosan avulla hyväksyt vain suojattujen yhteyksien käytön selaimessasi.

Firefox, Chrome

Privacy Badger: Suojaa yksityisyyttäsi estämälle verkkosivujen mahdollisuuden seurata selailuasi.

Firefox, Chrome

HUOM! Jokaisen lisäosan käyttäminen omalta osaltaan rajoittaa verkkoselaamiseen käytettyjä ominaisuuksia, joten käyttäjäkokemus saattaa muuttua eri palveluissa lisäosien käytön myötä.

BIOS

BIOS on joka tietokoneessa sijaitseva piiri, joka hoitaa matalantason toimia, jotta tietokoneen laitteisto sekä ohjelmisto keskustelisivat keskenään, sekä tietäisivät mitä tehdä. BIOS:n tulee päivityksiä, jotka parantavat laitteistojen yhteensopivuutta sekä suojaustasoa. BIOS ei päivity automaattisesti kuten käytetty käyttöjärjestelmä, vaan vaatii manuaalisia toimia.

Tarkista, BIOS:n ajantasaisuus. Katso BIOS:n päivitysohjeet.

Työaseman suojaus

Puhtaan näytön periaate

Puhtaan pöydän tai näytön periaatteella pääset alkuun, eli lähtökohtaisesti työpisteelle ei tulisi jättää valvomatta arkaluonteista tai kriittistä materiaalia. Jos et ole fyysisesti läsnä työasemallasi, lukitse päätelaite.

- **Lukitse päätelaite aina, jos jätät sen valvomatta.**

- **Huolehdi, että arkaluontoinen materiaali varastoidaan turvallisesti, kun sitä ei enää tarvita työskennellessä**

Turvalliseksi käytännöksi katsotaan, että käytät ns. peruskäyttäjää normaaliin verkkoselaamiseen ja työskentelyyn ja järjestelmänvalvojan tunnuksia esimerkiksi ohjelmien asentamiseen sekä poistamiseen. Tällä tavoin päätelaitteelle päässyt haittaohjelma ei pysty suoraan toimimaan järjestelmänvalvojan oikeuksin laitteellasi.

- **Luo itsellesi pääkäyttäjä sekä normaalikäyttäjä.**

  HUOM! Katso salalauseen hyvät periaatteet!

Salausmenetelmät

Nykyään organisaatioiden laitekanta koostuu paljonkin kannettavista tietokoneista, koska työ saattaa sisältää paljon matkustamista. Tällöin on hyvä varautua siihen, että laitteeseen kohdistuu suurempi riski tulla varastetuksi. Tietokoneen kovalevyn BitLocker-salaus, jonka avulla salausalgoritmi salaa levyn informaation pystyt viimekädessä varmistamaan, että kaikki informaatio on salattua.

- **Kytke Bitlocker salaus päälle. Katso ohjeet!**

Muistivälineen salaaminen käyttämällä esimerkiksi Veracrypt-salausohjelmistoa, pystyt varmistuman, että muistivälineessä olevaan dataan ei pääse suoraan käsiksi. Ohjelmiston avulla luot erillisen tiedoston, joka salataan salausalgoritmilla, jonka pystyt avaamaan vain luomallasi salalauseella.

- **Opettele käyttämään salausohjelmistoa, kuten Veracrypt ja käytä sitä muistivälineiden tai tiedostojen salaamiseen. Katso ohjeet.**

Muistivälineitä voidaan käyttää haittaohjelmien levitykseen sekä päätelaitteiden kaappaamiseen. Lisäksi muistilaitteiden katoamiseen ja vääriin käsiin joutuminen on riski, jota varten on järkevä puolustautua, jotta säilötty informaatio ei päädy vääriin käsiin.

Käytä yrityksesi tarjoamia muistivälineitä työntekoon äläkä missään nimessä käytä kadulta tai postiluukustasi tipahtanutta muistivälinettä työasemassasi.

Turvaohjelmistot

Työasemien suojaamiseen käytettäviä turvaohjelmistoja on monia ja valinnanvaraa löytyy. Organisaatioissa on yleisimmin hankittu päätelaitteille omat turvaohjelmistonsa. Turvaohjelmiston ajan tasalla pitäminen on tärkeää, koska ohjelmistojen tietokannat päivittyvät jatkuvasti uusien haittaohjelmien estämiseksi.

Yhden turvaohjelmiston käytön lisäksi toisen suojausteknologian käyttäminen voi parantaa haittaohjelmista suojautumista. Tähän voidaan soveltaa esimerkiksi Virustotal-palvelua, jonka avulla pystyt varmistamaan verkosta ladattavien tiedostojen turvallisuuden.

Virustotal-palvelussa on useiden eri turvaohjelmistojen valmistajien tietokantoja, joita palvelu käyttää tiedoston skannaamiseen.

Huom! Salassa pidettävien tai luottamuksellisten tiedostojen lataaminen Virustotal-palveluun vaarantaa tiedoston luottamuksellisuuden.

Tutustu ja kokeile Virustotal:iin.

Tietojenkäsittely

Tietoa on kahdessa muodossa sähköisenä, kuten työaseman kovalevyllä sekä fyysisessä muodossa, kuten asiakirjat.

- Fyysisen materiaalin osalta, kuten paperisessa muodossa oleva tieto tulisi säilyttää suojatussa ympäristössä, jossa riski sen joutumisesta asiattomien henkilöiden nähtäväksi tai käsiteltäväksi on pieni, kuten kassakaappi yms. Työpisteellä luottamuksellisen tai salaisen tiedon säilyttämistä tulee rajoittaa
- Sähköisessä muodossa tiedon säilyttämiseen tulee pohtia missä ja miten eli säilytys luotetussa sijainnissa sekä tiedoston salaaminen ovat hyviä käytänteitä.

Säilytä sinulle tai organisaatiollesi korvaamatonta tai luottamuksellista tietoa vain suojatuissa tiloissa tai tallennusmedioissa salattuna.

Tiedon siirtämiseen turvallisia kanavia pitkin, joko fyysisesti tai bitteinä on mietittävä mitä viestitään, millä viestintäkanavalla sekä vaadittu suojaustaso. Aluksi tulisi miettiä mitä tietoja tulet siirtämään tai lähettämään sekä niille sopiva tiedonsiirtokanava.

Tiedonsiirtokanava	**Suojausmenetelmä**
Sähköposti	Salatun sähköpostiyhteyden käyttö, kuten GPG/PGP, tai siirrettävän tiedoston kryptaus.
Yrityksen sisäiset viestintäkanavat	Suojattu yhteys sekä oikeuksienhallinta
Kirjekuori	Suojaus fyysisiltä vahingoilta.
Henkilökohtainen luovutus	Häiriötön sekä turvallinen tila.

✓ **Arvioi onko tarvetta tiedon salaukselle tiedonsiirron yhteydessä.**

Tietojen turvallinen käsittely vaatii suojatun ja turvallisen ympäristön sekä tarpeelliset toimenpiteet, jotta tieto pysyy sitä käsittelevien tahojen hallussa.

✓ **Käsittele luottamuksellisia tietoja varmistetussa suojatussa ympäristössä.**

Tiedon elinkaareen kuuluu sen turvallinen ja luottamuksellinen hävittäminen, joten tiedonsiirron sekä todetun käytön jälkeen tulee suorittaa tarvittavat hävitystoimenpiteet, jotta riskiä, että tieto jäisi leijumaan tai väärinkäytölle ei ole.

✓ **Asiakirjojen ja arvopapereiden hävitys tulisi tehdä turvallisessa ja luotetussa ympäristössä sekä siihen muotoon, että tiedon uudelleenkäyttöön tarvitaan merkittävästi vaivaa, kuten polttamalla tai silppuamalla.**

✓ **Sähköisissä muistivälineissä säilytetty luottamuksellinen tai salainen tieto tulisi formatoida ja yliajaa turvallisilla menetelmillä, siten, että tiedon palauttaminen on mahdotonta. Muistivälineiden fyysinen silppuaminen on myös vaihtoehto.**

Sähköiseen tiedon hävittämiseen muistivälineeltä voi käyttää esimerkiksi Eraser-ohjelmaa, joka yliajaa poistettavan tiedoston, siten että sen palauttaminen on käytännössä mahdotonta.

Varmuuskopiointi

Luottamuksellisen ja salaisen tiedon käsittelyn jälkeen tulisi asiakirjat saattaa suojattuun tilaan tai tuhota. Huomaa, että tärkeiden tietojen varmuuskopioinnilla vähennät tiedon aiheettomasta poistamisesta johtuvaa haittaa sekä katoamisen riskiä.

Varmuuskopioinnilla varmistut, että sinulle tärkeät tiedot ovat tallessa sekä kahdennetut. Suorita varmuuskopiointia säännöllisesti ulkoisille muistivälineille tai pilvipalveluihin sekä noudata organisaation mahdollisesti määrittelemiä menetelmiä varmuuskopioinnissa. Arvioi

samalla onko salausmenetelmien käyttöön tarvetta, eli onko esimerkiksi pilvipalveluun varmuuskopioitava informaatio luottamuksellisen tason tietoa.

Luo varmuuskopioita tärkeistä tiedoista, joita käsittelet tai haluat, että eivät katoa mahdollisten tietovälinevikojen ilmaantuessa.

Ei riitä, että tiedät ottaneesi varmuuskopiot, vaan ne tulee myös koestaa, jotta hätätilanteessa tietojen palauttaminen toimii vakuudella.

Koesta otetut varmuuskopiot.

Verkkokäyttäytyminen

Tärkein asia mikä kannattaa muistaa on se, että mieti kahdesti ennen kuin klikkaat ja opettele suodattamaan verkossa vastaantulevaa sisältöä, koska kaikki ei aina ole niin kuin kerrotaan tai näytetään. Loppujen lopuksi ihmisen oma käyttäytyminen sekä valinnat ovat suuressa roolissa verkossa olevien uhkien estämisessä.

Viestintäkanavat

Kyberrikollisuus on luova taiteenala, johon keksitään jatkuvasti uusia menetelmiä ja keinoja, joka tarkoittaa sitä, että puolustuksen täytyy olla menossa mukana eli mitä nopeammin erilaisten viestintäkanavien kautta saadaan tietoa päätelaitteiden käyttäjille erilaisista uhkista ja haavoittuvuuksista sen turvallisemmassa. Alla muutama esimerkki, viimeinen esimerkki on asioista tarkemmin kiinnostuneemmalle taholle.

Viestintäviraston kyberturvallisuuskeskus tarjoaa uutisointia löydetyistä haavoittuvuuksista sekä ohjeistuksia tavalliselle käyttäjälle ja organisaatioille. Haavoittuvuuksien ilmetessä kannattaa kurkata Lisätietoja-osio, joissa on tarkempaa tietoa kyseisestä aiheesta eri lähteistä.

Viestintäviraston kyberturvallisuuskeskus

F-Secure tarjoaa asiantuntija näkökulmia maailman turvallisuustilanteesta F-Securen näkökulmasta. Lisäksi yritys julkaisee omia tutkimuksiaan sekä tilanneraportteja tietoturvan tilasta yleisesti.

F-Securen uutisvirta

Security Affairs on EU:n verkko- ja tietoturvaviraston jäsenen ylläpitämä blogi, jossa pääkirjoittaja käsittelee tarkemmin esimerkiksi kooditasolla haittaohjelmia sekä haavoittuvuuksia.

Security Affairs

Seuraa, jotain mielekästä viestintäkanavaa tietoturvallisuuden tiimoilta.

Langattomat verkot

Avoimiin verkkoihin liittymistä kannattaa vältellä, koska verkkoon pystyy liittymään kuka tahansa lisäksi yhteyttä ei salata päätelaitteen ja tukiaseman välillä. Tällöin kuka tahansa pystyy kuuntelemaan ja tallentamaan verkkoliikennettä.

On kuitenkin huomioitavaa, että langattomien verkkojen WPA2-protokollan haavoittuvuuden takia kyseisellä menetelmällä suojatun langattoman verkon salaus on mahdollista purkaa.

Jos omistat langattoman tukiaseman, kytke tukiaseman asetuksista 802.11r-toiminto pois päältä, sekä pidä tukiasema päivitettynä.

Vältä avoimiin langattomiin verkkoihin liittymistä.

Ratkaisuna langattomien verkkojen osalta on suosia HTTPS-yhteyksiä toimivia verkkosivuja tai VPN-ratkaisun käyttöä, koska salaushaavoittuvuus ei ulotu verkkotekniikassa ylemmällä tasolla olevan salausmenetelmiin. VPN-ratkaisuja tarjoaa mm. F-Secure Freedome.

VPN-ratkaisuilla käytöllä kierrät myös langattomien verkkojen haavoittuvuuden sekä suojaat verkkoliikennettäsi.

Haittaohjelmien leviäminen

Haittaohjelmien leviäminen Internetin välityksellä on suhteellisen helppoja, jos käyttäjä on varomaton toimissaan. Yleisimmin haittaohjelmien tarkoitus on:

- Työasemien datan kerääminen ja sen lähettäminen eteenpäin
- Salasanojen ja tunnusten tai henkilötietojen kalastelu
- Vaurioittaa päätelaitteen ohjelmistoja
- Käyttää päätelaitteen laskentatehoa kryptovaluutan louhintaan
- Vakoilla päätelaitteen toimia ja varastaa käytettyjä tunnuksia
- Salata päätelaitteen kovalevy ja vaatia lunnaita salauksen purkuun

Tänä päivänä haittaohjelmat leviävät yleisimmin sähköpostin, epäilyttävien verkkosivujen sekä linkkien kautta tai ladattuasi ohjelmia verkosta, jonka kylkiäisinä saatat saada ilmaisohjelmia. Tosin luotettavienkin sivustojen saastuminen on olemassa riskinä. Yleisimmin yritetään jäljitellä, jotain luotetun toimijan verkkosivustoa ja sitä kautta urkkia tietoja.

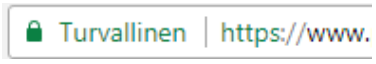
Lähihistorian esimerkki kryptovaluutanlouhintaan tarkoitetusta haittaohjelmasta terveysasemalla.

Verkkosivut

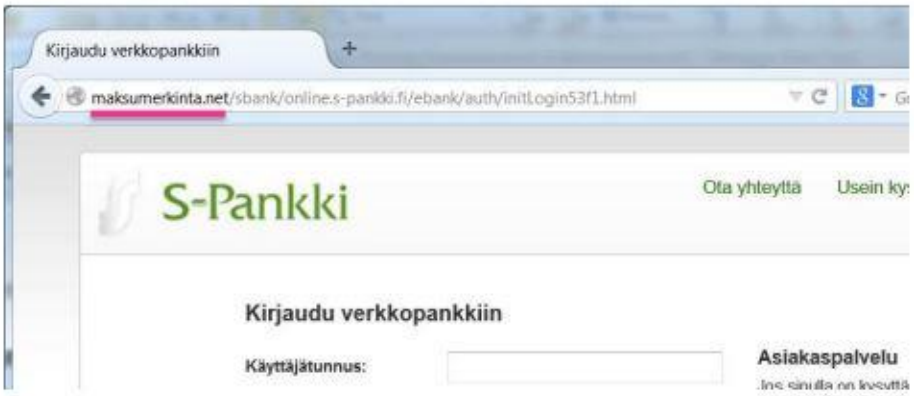
Verkkosivustot saattavat kerätä tietoa, käytetystä selaimesta, selain versiosta, käyttöjärjestelmästä, kauan sivuilla oltiin ja mitä klikattiin, joten pelkästään verkkosivuilla vierailu ajaa

monia taustaprosesseja, joilla saatat altistaa päätelaitteesi haittaohjelmille tai niiden levittämiseen. On siis mahdollista, että murretulla verkkosivulla on haittaohjelma taustalla, joka yrittää saastuttaa vierailijan selainta tai sen lisäosia.

✓ **Suosi salatun verkkoyhteyden omaavia eli HTTPS-yhteyksiä käyttäviä sivustoja, ja tarkasta aina osoitepalkin osoite, kuten alla.**



HTTPS suojattu yhteys.



S-pankin huijaussivusto. (Lähde: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/03/ttn201703091241.html)

Jos sinua kiinnostaa tietää verkkosivusta tarkempia tietoja käytä whois-palvelua, josta saat selville mm. verkkotunnuksen rekisteröijän ja ylläpitäjän. Verkkosivun luotettavuuden tarkastamiseen voit käyttää myös googlen sivuston selaussuoja analyysiä.

Whois-palvelu

Sivuston selaussuojatila

✓ **Älä klikkaa epäilyttäviä linkkejä tai ilmoituksia sähköpostista, Facebookista, Twitteristä tai muista yhteisöpalveluista, tai pikaviestimistä sekä opettele käyttämään sähköpostia turvallisesti.**

✓ **Jos havaitset, että päätelaitteellasi on haittaohjelma, irroita laitteen verkkokaapeli tai poistu langattomasta verkosta ja aja turvaohjelman skannaus. Jos olet työympäristössä ota myös yhteyttä organisaatiosi IT-tukeen.**

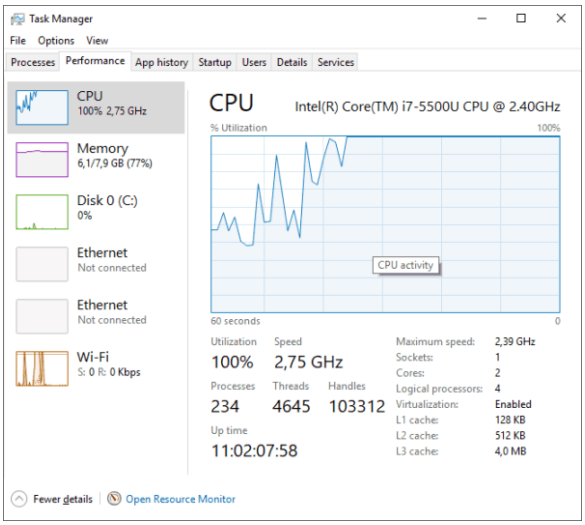
Kiristysohjelmat ja kryptovaluutan louhijat

Kiristysohjelmat ovat haittaohjelmia, jotka salaavat päätelaitteen kovalevyn ja vaativat lunnaita tietojen palauttamiseen. Suomessa Viestintävirasto, Poliisi sekä F-Secure ovat laatineet verkkosivun, jossa neuvotaan, miten toimit, jos joudut kontaktiin kiristysohjelmien kanssa.

Ransomware-ohjeet

Kiristyshaittaohjelman ilmentyessä työympäristössä irrota verkkokaapeli päätelaitteesta ja ota yhteyttä IT-tukeen.

Yleisimmin kryptovaluutan louhijat käyttävät päätelaitteen laskentatehoja, jotka pystyvät huomaamaan joko verkkosivun kuormituksen noustessa huomattavasti tai taustalla olevan tuntemattoman prosessin kuormituksen ollessa korkea. Varmista prosessin turvallisuus esimerkiksi googlettamalla tai konsultoimalla asiantuntijaa.



Tehtävienhallinnan näkymä (Lähde https://www.fortinet.com/blog/threat-research/cryptojacking-digging-for-your-own-treasure.html)

Tarkasta tehtävienhallinnasta resurssienkuorma, jos epäilet, että päätelaitteella on kryptovaluutan louhija. Sammuta prosessi ja aja turvaohjelma päätelaitteelle.

Sähköposti

Sähköposti on yksi kohde, josta normaalikäyttäjä pystyy suoraan omin silmin näkemään Internetin riskitekijöitä. Sähköpostiviestin kanssa kannattaa olla erityisen kriittinen viestejä kohtaan, joita vastaanotat.

F-Secure listasi vuoden 2017 suosituimmat väärennetyt lähettäjäyhtiöt roskaposteissa koko maailmassa sekä pohjoismaissa: Katso tästä

Yleisimmät huijausviestit, jota todennäköisesti tulet saamaan sähköpostiisi käsittelevät aiheita:

- Rikastuminen eli olet voittanut arvonnassa, lotossa, kisassa jne.
- Nigerialaiskirjeet eli ryhdy liikekumppaniksi ja saa suuria palkkioita
- Seuranhaku
- Terveystuotteet yleisimmin Viagra
- Henkilötietokysely
- Jonkin palvelun tilisi on kaapattu ja lähetä tunnuksesi eteenpäin

Arvioi vastaanotettuja sähköpostiviestejä ainakin seuraavien ominaisuuksien kautta:

- Onko viesti täynnä kirjoitusvirheitä tai kirjoitusasu on kehnoa suomen- tai englannin kieltä
- Viestin mukana saattaa olla liitetiedosto pdf, jpeg, gif, docx, exe, cmd, bat, jota pyydetään avaamaan.
- Viesti sisältää linkin, jota viestin mukaan pitäisi klikata.
- Lähettäjän sähköpostiosoite on todella epäilyttävän oloinen tai siinä on yritetty jäljitellä. jotain organisaatiota esimerkiksi tim6672562@gas123df.org tai aspa451@feikkaus.eu
- Viestissä yritetään jäljitellä esimerkiksi organisaatioiden, kuten pankkien, poliisin, matkatoimistojen graafista ulkonäköä, mutta laaduttomin lopputuloksin.
- Jos et oikeasti ole ollut kontaktissa tai odota kontaktia johonkin organisaatioon tai henkilöön ja saat yhteydenoton, jossa pyydetään lähettämään lisätietoja itsestäsi, on mahdollista, että viesti on huijaus.
- Jos et ole osallistunut arvontoihin, et ole myöskään voinut voittaa mitään.

Viestintäviraston teettämän julkaisun Tietoturvan vuosi 2017 mukaan sähköpostin mukana levitettävät liitetiedostot, kuten Word-dokumentti olivat ylivoimaisesti suosituin tapa levittää haittaohjelmia.

✓ **Älä avaa huijausviestiksi tai roskapostiksi arvioimaasi viestiä.**

✓ **Muista, että rahalaitokset, viranomaiset tai muut asialliset tahot eivät koskaan kysele sinun tilitietojasi, tunnuksia tai muuta salassa pidettäviä materiaaleja sähköpostin välityksellä.**

Tiedostojen lataaminen

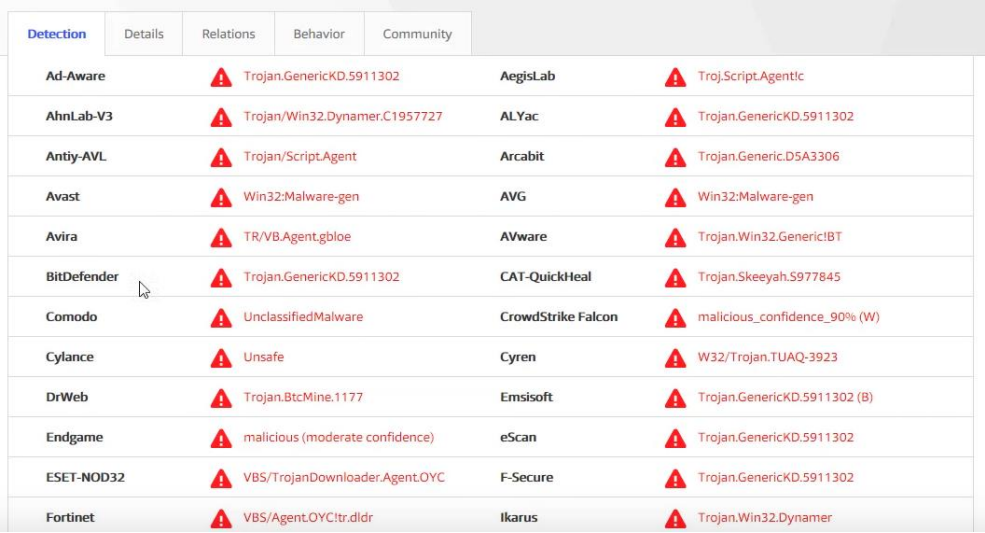
Verkosta ladattavien tiedostojen luotettavuutta ei pystytä pelkästään lähteen perusteella päättelemään vaan olisi käytettävä vaihtoehtoista palvelua tiedoston turvallisuuden takaamiseksi.

✓ **Jos lataat ohjelmistoja tai tiedostoja verkosta, voit skannata sen Virustotal-palvelun kautta.**

Ota huomioon, että työskennellessäsi yrityksissä saattaa käsiteltävänäsi olla asiakasmateriaalia sekä luottamuksellista tietoa, jolloin Virustotal-palvelun käyttö ei ole suotavaa, koska tavoitteena on varjella salassa pidettävää sekä luottamuksellista materiaalia ulkopuolisilta.

Jos skannauksen lopputuloksessa ilmenee ongelmia älä jatka tiedoston käsittelyä. Jos lopputuloksena on yhden tai kahden palvelun ilmoitus haittaohjelmista ota selvää onko kyseessä väärä hälytys esimerkiksi lukemalla yhteisön arviot.

Pahimmassa tapauksessa tulos on jotain alla olevan näköistä, jolloin olisi paras poistaa tiedosto ja ajaa turvatarkastus päätelaitteelle.



Detection	Details	Relations	Behavior	Community

Ad-Aware	Trojan.GenericKD.5911302	AegisLab	Troj.Script.Agent!c
AhnLab-V3	Trojan/Win32.Dynamer.C1957727	ALYac	Trojan.GenericKD.5911302
Antiy-AVL	Trojan/Script.Agent	Arcabit	Trojan.Generic.D5A3306
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/VB.Agent.gbloe	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.5911302	CAT-QuickHeal	Trojan.Skeeyah.S977845
Comodo	UnclassifiedMalware	CrowdStrike Falcon	malicious_confidence_90% (W)
Cylance	Unsafe	Cyren	W32/Trojan.TUAQ-3923
DrWeb	Trojan.BtcMine.1177	Emsisoft	Trojan.GenericKD.5911302 (B)
Endgame	malicious (moderate confidence)	eScan	Trojan.GenericKD.5911302
ESET-NOD32	VBS/TrojanDownloader.Agent.OYC	F-Secure	Trojan.GenericKD.5911302
Fortinet	VBS/Agent.OYC!tr.dldr	Ikarus	Trojan.Win32.Dynamer

Virustotalin skannaama troijalainen

Sosiaalinen media

Sosiaalisessa mediassa ilmenee samalla tavalla uhkia, jotka kohdistuvat esimerkiksi käyttäjien henkilötietojen kalasteluun sekä identiteettivarkauksiin sekä haittaohjelmien levittämiseen. Mieti, millaista materiaalia haluat julkaista sosiaalisessa mediassa, koska materiaalin varastaminen on helppoa ja sen avulla voidaan luoda väärennettyjä profiileja. Yksityisyyteen kannattaa panostaa, koska oletuksena palvelut asettavat profiilisi mahdollisimman avoimeksi, jolloin vastuu jää sinulle päättää, kuinka avoimesti haluat jakaa tietojasi.

- ✓ **Jos saat tuntemattomalta ihmiseltä kaveripyynnön, harkitse kolmesti haluatko hyväksyä pyynnön.**
- ✓ **Selvitä millaiset yksityisyysasetukset palvelussa on käytössä ja pohdi kuinka avoimesti haluat näyttäytyä maailmalle.**
- ✓ **Harkitse, mitä haluat mainita työpaikastasi sekä ota selvää, kuinka työpaikalla suhtaudutaan sosiaaliseen mediaan.**
- ✓ **Sosiaalisen median kautta pystytään jakamaan haitallisia linkkejä sekä tiedostoja, joiden välttämiseksi harkitse mitä lataat ja mitä linkkiä painat.**

Verkossa löytyvä yhteisöpalvelu Terms of Service: Didint´t Read, kokoaa eri palveluiden käyttöehtojen arvioita tietojenkäsittelyyn ja jakamiseen liittyen. Palvelussa pystyt itse arvioimaan, millaisiin asioihin palvelun käyttöön liittyen olet antanut tai tulet antamaan hyväksynnän.

Mobiililaitteet

Puhelimiin ladattavia sovelluksia kannattaa pitää päivitettynä, kuten muissakin päätelaitteissa, sekä ladata sovelluksia vain puhelimen asennetusta sovelluskaupasta.

Mobiililaitteiden käytön lisääntyessään entisestään asettaa se myös uusia vaaroja tietoturvallisuuden osalta. Älypuhelin on aivan samanlainen tietokone kuin työssäsi käytettävä kannettava tietokone tai yksityisyyskäyttöön tarkoitettu pöytätietokone. Älypuhelimeen pätevät samanlaiset periaatteet kuin muidenkin päätelaitteiden kanssa käyttöturvallisuuden osalta:

- ✓ **Vaihda SIM-kortin salasana johonkin muuhun ja pidempään kuin 0000 tai 1234.**
- ✓ **Aseta puhelimeen näytönlukitus automaattiseksi sekä vahva salasana lukituksen poistoon.**

Mobiililaitteille yleisimmät tavat levittää haittaohjelmia ovat huijausviestit, joissa yleisimmin ohjeistetaan esimerkiksi antamaan pankkitilitunnuksia tai henkilötietoja, jonkin verkkolinkin takaa.

Nykyään myös erilaiset huijauspuhelut ovat arkipäivää, joissa tuntemattomasta numerosta soitetaan ja esittäydytään poliisina tai muuna virkailija ja urkitaan tilitietoja. Huijaustilanteet on tunnistettava ja välttää haksahtamasta ansaan.

Kuten, jo Mitä? -osiossa viitattiin F-Securen julkaisuun erityisesti Android-version omaavat mobiililaitteet ovat haittaohjelmien kohteena, joten turvaohjelmiston käyttö mobiililaitteella on harkittavaa.

- ✓ **Turvasovelluksen hankintaa suositellaan hankittavaksi erityisesti työpuhelimen käyttöön liittyen.**
- ✓ **Jos puhelimeesi tarttuu haittaohjelma tarkista turvaohjelmalla puhelimesi, palauta tehdasasetukset ja jos kyseessä on työpuhelin ota yhteyttä IT-tukeen.**
- ✓ **Jos puhelimesi joutuu hukkaan tai varastetaan, paikannussovelluksen avulla pystyt paikantamaan ja tyhjentämään tarvittaessa puhelimen.**

Salalauseet

Aivan aluksi pohdi, mitkä tunnukset ovat sinulle prioriteeteiltaan kaikkein tärkeimpiä sekä tee yhteenvetoa montako käyttäjätunnusta sinulla on käytössäsi. Priorisoinnin taustalla on ajatus siitä, että on olemassa palveluita, joiden tunnuksien taustalla on kriittisiä asioita tai yhdistettyjä palveluita, kuten sähköpostitililläsi.

Usein myös muistikapasiteetti tulee vastaan salasanojen muistamisessa, kun palveluita alkaa olemaan kymmeniä, joka altistaa samojen salasanojen käyttöön sekä niiden ylös kirjoittamisen muistilapulle tai vastaavalle.

Salalauseen muodostaminen

Salasanan käyttämisen korvaamiseksi olisi turvallisempaa luoda itselle salalauseita. Lause on helpompi muistaa sekä ei ole niin helposti murrettavissa ”brute force” sekä sanakirjahyökkäyksillä.

Salalauseen muodostamisessa olisi kuitenkin hyvä muistaa muutama pointti:

- Käytä Isoja ja pieniä kirjaimia ja numeroita ja mahdollisesti erikoismerkkejä
- Luo lause, jossa ei ole mitään järkeä ja on riittävän pitkä vähintään 15 merkkiä
- Käytä apuna halutessasi apuohjelmia lauseen muodostamisessa, kuten https://jiippana.kapsi.fi/

✓ **Suosi salalauseita salasanojen sijaan.**

✓ **Aina kun otat käyttöön uuden laitteen, tunnuksen palveluun tai minne tahansa, muuta oletussalasana pikimmiten!**

Salalauseet ovat henkilökohtaisia ja niiden jakaminen ei ole suotavaa eikä järkevää lisäksi niiden säilyttäminen lapuilla tai puhelimen muistiossa ovat riskialttiita menetelmiä niiden suojelemiseen. Jos sinun on pakko säilyttää salalausetta jossain, puolita salalause niin, että koko lausetta ei ole yhdessä muistiossa tai lapulla.

Usein palveluissa pyydetään luomaan turvakysymyksiä tai vinkkejä sen varalta, jos käyttäjän salasana on unohtunut tai haluat uuden salasanan. Tällaisiin kysymyksiin ja vinkkeihin ei pidä vastata rehellisesti, koska on mahdollista, että murtautuja pystyy urkkimaan sukulaisesi, ystäväsi, koirasi nimen tai muuta vastaavaa, jos olet esimerkiksi maininnut sosiaalisessa mediassa asiasta.

✓ **Valehtele turvakysymyksissä äläkä anna vinkkejä salasanaan.**

Salasananhallinta ohjelmisto

Helpoin tapa vapauttaa muistikapasiteettiä ja aikaa salasanoilta on luoda salattu tietokanta salasananhallinta ohjelmistolla, jonka avulla sinun ei tarvitse muistaa kuin yksi salalause, jolla pystyt avaamaan tietokannan.

Yleisimpiä hallinta ohjelmistoja ovat:

Keepass Password Safe

KeePassX

Password Safe

Ohjelmisto luo käyttöösi tietokannan, joka kryptataan salausalgoritmilla sekä halutessasi muilla salausmenetelmillä. Tietokantaan pääsee käsiksi pääsalasanalla. Ohjelmiston avulla luot halutessasi niin monimutkaisen ja pitkän salasanan, palveluihin kuin vain haluat. Huomioi, mitä merkkejä palvelu sallii salasanan käytössä.

On kaksi asiaa mitä tulee muistaa ohjelman käyttöön liittyen:

1. Luo tarpeeksi vahva salalause tietokannan avaamiseen.
2. Ole tarkka, minne liität salasanasi.

Perusteena edellisiin on se, että tietokantaasi suojaa yksi salalause, joten panosta siihen, koska sen takana ovat luonnollisesti kaikkien muiden palveluiden salasanat. Toisena salasanan liittäminen väärään palkkiin saattaa asettaa tunnuksen vaaraan, jos työasemassa on haittaohjelma tai verkkosivun toimintaa tarkkaillaan.

✓ **Opettele käyttämään salasananhallinta ohjelmistoa.**

Ohjelmiston avulla luotua tietokanta olisi hyvä varmuuskopioida pilveen tai erilliselle muistivälineelle. Lisäsuojan antamiseksi tietokannan salaamista Truecrypt-ohjelmalla tai vastaavalla kannattaa harkita.

✓ **Muista varmuuskopioida tietokanta sekä suojata tallennusväline tai tietokanta.**

Kaksivaiheinen tunnistus

Kaksivaiheisessa tunnistautumisessa yleensä lähetetään puhelimeen joka kerta vaihtuva koodi, jolla pääset kirjautumaan palveluun. Kaksivaiheinen tunnistautuminen on tapa, jolla varmistat, että käyttämääsi palveluun ei ole mahdollista kirjautua pelkästään käyttäjätunnus ja salasana parilla.

Lisäksi kaksivaiheisella tunnistautumisella saat tietoosi, onko joku muu yrittänyt kirjautua tunnuksillasi palveluun, joka indikoi sitä, että salasana tulisi vaihtaa pikimmiten.

Huomaa, että turvautumalla pelkästään kaksivaiheiseen tunnistautumiseen ja heikkoon salalauseeseen altistaa riskiä joutua hyökkäyksen kohteeksi. Jos hyökkääjä tietää tunnuksen, salalauseesi sekä puhelinnumerosi, voi hän lähettää ennakoivasti ”tunnistautumisviestin” puhelimeesi ja varomattomasti saatat joutua uhriksi. Tarkempaa tietoa esimerkkitapauksesta.

✓ **Suosi palveluissa kaksivaiheista tunnistautumista, jos siihen on mahdollisuus.**

Miksi?

Päivitykset

Miksi päivittäminen on niin tärkeää ja mitä hyötyä siitä on minulle:

- ✓ **Päivitysten ansiosta pystyt parantamaan ohjelmistojen vakautta ja poistamaan vanhoja haavoittuvia ominaisuuksia.**
- ✓ **Käyttökokemus paranee, jolloin mahdolliset bugit ja virheet korjautuvat.**
- ✓ **Suojaat itsellesi sekä yritykselle tärkeitä resursseja vähentäen näin riskiä joutua tietomurron kohteeksi.**

Mitä voi tapahtua, jos jätän päivitykset huomiotta:

- ✗ **Henkilökohtaisen tai luottamuksellisen tiedon katoaminen sekä sen hyväksikäyttö**
- ✗ **Ohjelmiston tai laitteiston vaurioituminen.**
- ✗ **Haavoittuvuuden hyväksikäytön myötä saatat levittää haittaohjelmia muihin järjestelmiin verkossa.**

Työaseman suojaus

Minkä takia työaseman suojaamiseen kannattaa kuluttaa aikaa sekä työpanosta?

- ✓ **Varmistut, että turvallisien menettelyjen kautta itsellesi, asiakkaallesi tai organisaatiollesi tärkeä informaatio pysyy luottamuksellisena.**
- ✓ **Työskennellessäsi organisaatiossa suojelet sekä vahvistat työpaikkasi mainetta turvallisena toimijana.**
- ✓ **Vähennät riskitekijöitä, joilla tietovälineiseen kohdistuu turvauhkia.**

Millaisia asioita saattaa tapahtua, jos työaseman suojausmenetelmiä ei ole otettu huomioon tai toteuttaminen ontuu?

- ✗ **Työasemaa voidaan käyttää hyväksi, vaikkapa bottiverkkona tai kryptovaluutan louhinnassa.**
- ✗ **Kasvattaa riskiä tietomurtoihin ja kriittisen tiedon vuotamiseen.**
- ✗ **Organisaatioon kohdistuu maineriski kasvaa, jos sen tietojärjestelmiin kohdistuu tietovuoto.**

Tietojenkäsittely

Alle on luoteltu asioita, jotka saattavat resonoida lukijaa kohti hallittuun tietojenkäsittelyyn.

- ✓ **Riski tiedon väärinkäytölle vähenee.**
- ✓ **Informaatio pysyy luottamuksellisena sekä eheänä sen koko elinkaaren ajan.**
- ✓ **Varmuuskopioinnilla suojaudut ennakoivasti mahdollisia ongelmatilanteita varten.**

Alla on näkökulmia, joita saattaa nousta esille, kun toimit huolimattomasti tietojenkäsittelyn yhteydessä.

- ✗ **Epävarmuustekijät tiedon luottamuksellisuuden säilyttämiseen kasvavat.**
- ✗ **Riskit informaation vuodolle, väärinkäytölle sekä katoamiseen kasvavat.**
- ✗ **Tiedonkäsittelyn strukturoimattomuus saattaa johtaa sekaannuksiin ja saattaa aiheuttaa toiminnallisia häiriöitä.**

Verkkokäyttäytyminen

Päätelaitteen käyttäjän käyttäytyminen verkossa on tärkein rajapinta ja portti tiedonurkkijoille ja haittaohjelmille, joten vaikutuksen laajuus voi olla suurikin, jos esimerkiksi organisaation järjestelmät saastuvat tai henkilökohtaisia materiaaleja ja tietoja käytetään hyväksi. Saatat joutua sosiaalisen manipuloinnin kohteeksi, jolloin hallussasi tai tiedossasi olevia salassa pidettäviä tai luottamuksellisia tietoja käytetään hyväksi.

Mitä asioita turvaat, kun toimit turvallisesti verkossa:

- ✓ **Turvallisten käytäntöjen avulla vähennät riskiä, että päätelaitteesi saastuu ja itsellesi tai organisaatiollesi tärkeitä materiaaleja ja tietoja ei pääse vuotamaan.**
- ✓ **Ennaltaehkäiset vaikeita ongelmatilanteita ja rikollista toimintaa.**
- ✓ **Ylläpidät turvallista työskentelyilmapiiriä.**

Miten huolimaton ja varomaton toiminta saattaa vaikuttaa itseesi ja työympäristöösi:

- ✗ **Kasvattaa riskiä laitteiston saastumiseen ja tiedon vuotamiseen, väärinkäyttöön ja tuhoutumiseen.**
- ✗ **Asettaa muut saman verkon tai palveluiden käyttäjät vaaraan.**
- ✗ **Edesauttaa rikollisen sekä työskentelyä haittaavan toiminnan jatkuvuutta.**

Salalauseet

Tunnistautumistiedot eli tässä tapauksessa salasanat ovat todentamismenetelmä, jolla annetaan oikeuksia palveluihin tai käyttölupa. Salasanan murtaminen on yleisin menetelmä, jolla hakkerit murtautuvat päätelaitteisiin ja käyttäjätileihin. Siksi myös vahvan salasanan sekä salasanojen suojausmenetelmien käyttö on tarpeellista. Alla kolme esimerkki pointtia miksi tulisi panostaa vahvaan salalauseeseen, suojausmenetelmiin ja hallintaan.

✓ **Käyttämällä vahvoja salalauseita vahvistat suojautumistasi mahdollisia murtoyrityksiä laitettasi ja tiliäsi vastaan.**

✓ **Käyttämällä salasananhallinta ohjelmistoa vapautat muistikapasiteettiäsi sekä parannat salasanojen turvallisuutta.**

✓ **Luot työympäristöön sekä yksityiselämääsi vakautta ja turvaa käyttämällä aina vahvinta mahdollista tunnistautumismenetelmää.**

Alla kolme esimerkkikohtaa, jota voi tapahtua huonon salasanan tai sen hallinnan seuraamuksena.

✗ **Huolimaton salasanojen käyttö sekä hallinta altistavat käyttökohteesta riippuen laitteen kaappaukseen, rahalliseen menetykseen tai henkiseen kärsimykseen.**

✗ **Riski tietomurtoa kohtaan kasvaa ja näin ollen työympäristön turvallisuus vaarantuu.**

✗ **Riski haittaohjelmien leviämiseen sekä päätelaitteiden väärinkäyttöön kasvaa.**

Tarkastuslista

Päivitykset	
Tarkasta käyttöjärjestelmäsi, ohjelmistosi, selaimesi sekä sen lisäosien ajantasaisuus.	
Tarkista BIOS:n ajantasaisuus.	
Työaseman suojaus	
Lukitse päätelaite aina, jos jätät sen valvomatta.	
Huolehdi, että arkaluontoinen materiaali varastoidaan turvallisesti, kun sitä ei enää tarvita työskennellessä.	
Luo itsellesi pääkäyttäjä sekä normaalikäyttäjä, joille luot turvalliset salalauseet.	
Kytke Bitlocker salaus päälle. Katso ohjeet.	
Käytä organisaatiosi tarjoamia muistivälineitä työntekoon.	
Opettele käyttämään salausohjelmistoa, kuten Veracrypt ja käytä sitä muistivälineiden salaamiseen. Katso ohjeet.	
Tietojenkäsittely	
Säilytä sinulle tai organisaatiollesi korvaamatonta tai luottamuksellista tietoa vain suojatuissa tiloissa tai tallennusmedioissa salattuna.	
Arvioi onko tarvetta tiedon salaukselle tiedonsiirron yhteydessä.	
Käsittele luottamuksellisia tietoja varmistetussa suojatussa ympäristössä.	

Asiakirjojen ja arvopapereiden hävitys tulisi tehdä turvallisessa ja luotetussa ympäristössä sekä siihen muotoon, että tiedon uudelleenkäyttöön tarvitaan merkittävästi vaivaa, kuten polttamalla tai silppuamalla.	
Sähköisissä muistivälineissä säilytetty luottamuksellinen tai salainen tieto tulisi formatoida ja yliajaa turvallisilla menetelmillä, siten, että tiedon palauttaminen on mahdotonta. Muistivälineiden fyysinen silppuaminen on myös vaihtoehto.	
Luo varmuuskopioita tärkeistä tiedoista säännöllisesti ja koesta otetut varmuuskopiot.	
Verkkokäyttäytyminen	
Seuraa, jotain mielekästä viestintäkanavaa tietoturvallisuuden tiimoilta.	
Vältä avoimiin langattomiin verkkoihin liittymistä.	
Harkitse tarvitsetko VPN-ratkaisuja liikennöidessäsi verkossa.	
Arvioi vastaanotettuja sähköpostiviestejä ainakin seuraavien ominaisuuksien kautta: • **Onko viesti täynnä kirjoitusvirheitä tai kirjoitusasu on kehnoa suomen- tai englannin kieltä** • **Viestin mukana saattaa olla liitetiedosto pdf, jpeg, gif, docx, exe, cmd, bat, jota pyydetään avaamaan.** • **Viesti sisältää linkin, jota viestin mukaan pitäisi klikata.** • **Lähettäjän sähköpostiosoite on todella epäilyttävän oloinen tai siinä on yritetty jäljitellä. jotain organisaatiota esimerkiksi tim6672562@gas123df.org tai aspa451@feikkaus.eu** • **Viestissä yritetään jäljitellä esimerkiksi organisaatioiden, kuten pankkien, poliisin, matkatoimistojen graafista ulkonäköä, mutta laadutto-min lopputuloksin.** • **Jos et oikeasti ole ollut kontaktissa tai odota kontaktia johonkin organisaatioon tai henkilöön ja saat yhteydenoton, jossa pyydetään lähettämään lisätietoja itsestäsi, on mahdollista, että viesti on huijaus.**	
Älä avaa huijausviestiksi tai roskapostiksi arvioimaasi viestiä.	
Muista, että rahalaitokset, viranomaiset tai muut asialliset tahot eivät koskaan kysele sinun tilitietojasi, tunnuksia tai muuta salassa pidettäviä materiaaleja sähköpostin välityksellä.	
Suosi salatun verkkoyhteyden omaavia eli HTTPS-yhteyksiä käyttäviä sivustoja	
Tarkista aina selaimen osoitepalkin osoite verkossa liikkuessasi.	
Älä klikkaa epäilyttäviä linkkejä tai ilmoituksia sähköpostista, Facebookista, Twitteristä tai muista yhteisöpalveluista tai pikaviestimistä.	
Jos havaitset, että päätelaitteellasi on haittaohjelma, irroita laitteen verkkokaapeli tai poistu langattomasta verkosta ja aja turvaohjelman skannaus. Jos olet työympäristössä ota yhteyttä organisaatiosi IT-tukeen.	
Muista varmentaa verkosta ladattujen tiedostojen turvallisuus, jollain menetelmällä, kuten Virustotal-palvelun avulla.	
Kiristyshaittaohjelman ilmentyessä työympäristössä irrota verkkokaapeli päätelaitteesta ja ota yhteyttä IT-tukeen.	
Jos saat tuntemattomalta ihmiseltä kaveripyynnön, harkitse kolmesti haluatko hyväksyä pyynnön.	
Selvitä millaiset yksityisyysasetukset palvelussa on käytössä ja pohdi kuinka avoimesti haluat näyttäytyä maailmalle.	
Harkitse, mitä haluat mainita työpaikastasi sekä ota selvää, kuinka työpaikalla suhtaudutaan sosiaaliseen mediaan.	

Sosiaalisen median kautta pystytään jakamaan haitallisia linkkejä sekä tiedostoja, joiden välttämiseksi harkitse mitä tiedostoja lataat tai linkkejä painat.	
Vaihda SIM-kortin salasana johonkin muuhun ja pidempään kuin 0000 tai 1234, jotka eivät ole hyviä salasanoja.	
Aseta puhelimeen näytönlukitus automaattiseksi sekä vahva salasana lukituksen poistoon.	
Turvasovelluksen hankintaa suositellaan hankittavaksi erityisesti työpuhelimen käyttöön liittyen.	
Jos puhelimeesi tarttuu haittaohjelma tarkista turvaohjelmalla puhelimesi, palauta tehdasasetukset tai jos kyseessä on työpuhelin ota yhteyttä IT-tukeen.	
Jos puhelimesi joutuu hukkaan tai varastetaan, paikannussovelluksen avulla pystyt paikantamaan ja tyhjentämään tarvittaessa puhelimen.	
Salalauseet	
Suosi salalauseita salasanojen sijaan.	
Aina kun otat käyttöön uuden laitteen, tunnuksen palveluun tai minne tahansa, muuta oletussalasana pikimmiten.	
Valehtele tunnusten turvakysymyksissä äläkä anna vinkkejä salasanaan.	
Opettele käyttämään salasananhallinta ohjelmistoa.	
Muista varmuuskopioida salasananhallinta ohjelmiston tietokanta sekä suojata tallennusväline tai tietokanta.	
Käytä palveluissa kaksivaiheista tunnistautumista, jos siihen on mahdollisuus.	